IBM **Security**

X-Force Threat Intelligence Index 2022

IBM

Contents

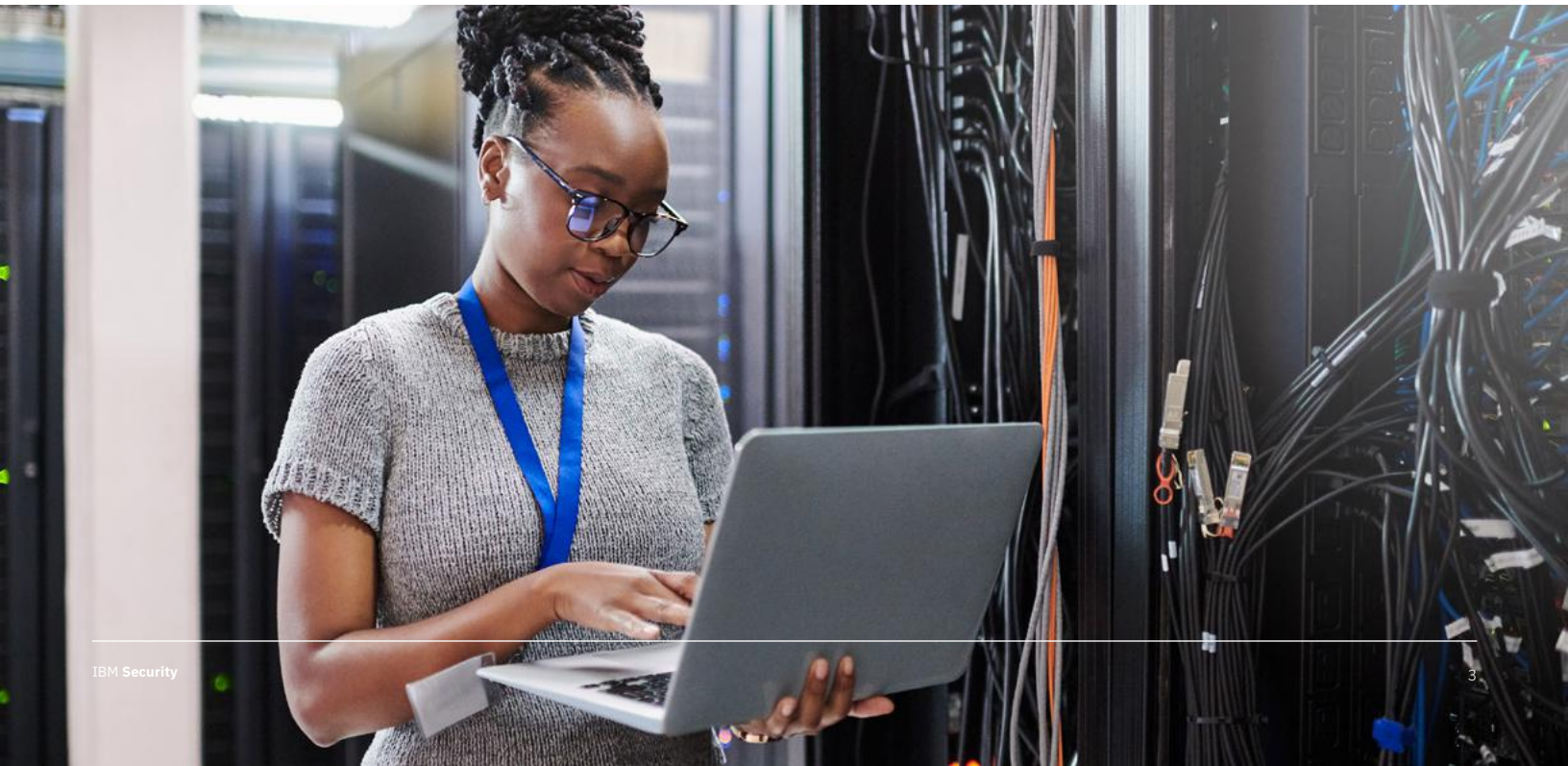
Executive summary

The world continues to grapple with a lasting pandemic, shifts to work-from-home and back-to-office, and geopolitical changes spawning a constant drone of mistrust. All of this equates to chaos, and it is in chaos that cybercriminals thrive. In 2021, IBM Security® X-Force® saw how threat actors opportunistically used a shifting landscape to adopt tactics and techniques to successfully infiltrate organizations across the globe.

The IBM Security X-Force Threat Intelligence Index maps new trends and attack patterns we observed and analyzed from our data—drawing from billions of datapoints ranging from network and endpoint detection devices, incident response (IR) engagements, domain name tracking and more. This report represents the culmination of that research based on data collected from January to December 2021.

We offer these findings as a resource to IBM clients, researchers in the security industry, policy makers, the media and to the broader community of security professionals and business leaders.

Given the volatile landscape and the evolution of both threat types and threat vectors, you need threat intelligence insights to stay ahead of attackers and fortify your critical assets more than ever.



Report highlights

Top attack type: Ransomware was again the top attack type in 2021, although the percentage of attacks X-Force remediated that were ransomware decreased nearly 9% year-over-year. REvil—a ransomware type X-Force also refers to as Sodinokibi—was the most common ransomware strain X-Force observed for a second year, making up 37% of all ransomware attacks, followed by Ryuk at 13%. Law enforcement activity has probably been the primary force driving down ransomware and IoT botnet attacks in 2021, but this does not preclude a potential resurgence in 2022.

Supply chain vulnerabilities: Supply chain security was pushed to the forefront of government and policymakers' attention, with the Biden administration's executive order on cybersecurity, and guidance from the U.S. Department of Homeland Security, CISA, and NIST doubling down on zero trust guidance. These guidelines put a spotlight on vulnerabilities and trusted relationships. Vulnerability exploitation was the top initial attack vector in manufacturing, an industry grappling with the effects of supply chain pressures and delays.

Most phished brands: X-Force closely tracked how cybercriminals are using phishing kits throughout 2021, and our research revealed that Microsoft, Apple and Google were the top three brands criminals attempted to mimic. These mega brands were used repeatedly in phishing kits, with attackers likely seeking to capitalize on their popularity and the trust many consumers place in them.

Top threat groups: Suspected Iranian nation-state threat actor ITG17 (MuddyWater), cybercriminal group ITG23 (Trickbot), and Hive0109 (LemonDuck) were some of the most active threat groups X-Force intelligence analysts observed in 2021. Threat groups worldwide were seeking to augment their prowess and infiltrate more organizations. Malware they used was embedded with greater defense-evasion techniques, in some cases hosted via cloud-based messaging and storage platforms to get through security controls. These platforms were abused to hide command and control communication in legitimate network traffic. Threat actors also continued to develop Linux versions of malware, to enable them to cross over to cloud environments more easily.

Key stats

21%

Ransomware share of attacks
Ransomware was the number one attack type observed by X-Force last year, decreasing to 21% of attacks from 23% in the previous year. REvil ransomware actors (aka Sodinokibi) were responsible for 37% of all ransomware attacks.

17 months

Average time before a ransomware gang rebrands or shuts down
Ransomware gangs studied by X-Force had an average lifespan of 17 months before rebranding or disbanding. REvil, one of the most successful gangs, shut down in October 2021 after 31 months (two and a half years).

41%

Percentage of attacks exploiting phishing for initial access
Phishing operations emerged as the top pathway to compromise in 2021, with 41% of incidents X-Force remediated using this technique to gain initial access.

33%

Increase in the number of incidents caused by vulnerability exploitations from 2020 to 2021
Four out of the top five vulnerabilities exploited in 2021 were new vulnerabilities, including the Log4j vulnerability CVE-2021-44228—which was ranked number two, despite only being disclosed in December.

3X

Click effectiveness for targeted phishing campaigns that add phone calls
The click rate for the average targeted phishing campaign was 17.8%, but targeted phishing campaigns that added phone calls (vishing or voice phishing) were three times more effective, netting a click from 53.2% of victims.

146%

Increase in Linux ransomware with new code

The percentage of Linux ransomware with unique (new) code increased year-over-year by 146%, according to Intezer, indicating an increase in the level of Linux ransomware innovation.

#1

Manufacturing industry rank for attacks

Manufacturing replaced financial services as the top attacked industry in 2021, representing 23.2% of the attacks X-Force remediated last year. Ransomware was the top attack type, accounting for 23% of attacks on manufacturing companies.

61%

Manufacturing share of compromises on OT-connected organizations

Sixty-one percent of incidents at OT-connected organizations last year were in the manufacturing industry. In addition, 36% of attacks on OT-connected organizations were ransomware.

2,204%

Increase in reconnaissance against OT

Attackers increased their reconnaissance of SCADA Modbus OT devices accessible via the internet by 2,204% between January and September 2021.

74%

Share of IoT attacks originating from Mozi botnet

In 2021, attacks against IoT devices originated from the Mozi botnet 74% of the time.

26%

Share of global attacks that targeted Asia

Twenty-six percent of all attacks had targets in Asia in their crosshairs. Asia was the most attacked geography of 2021.

Top attack types

For the purposes of this report, we categorize attack types by the *end goal* an attacker is seeking to achieve once they have gained access to a victim's network. Attack types differ from initial infection vectors, with the latter being the initial method of entry into a network.

As examples, some attack types include ransomware, data theft, and BEC, based on the end goal of the threat actor's operation. Examples of initial infection vectors include phishing, using stolen credentials, and vulnerability exploitation.

The following sections provide details and data on the most prolific attack types our data revealed in 2021.

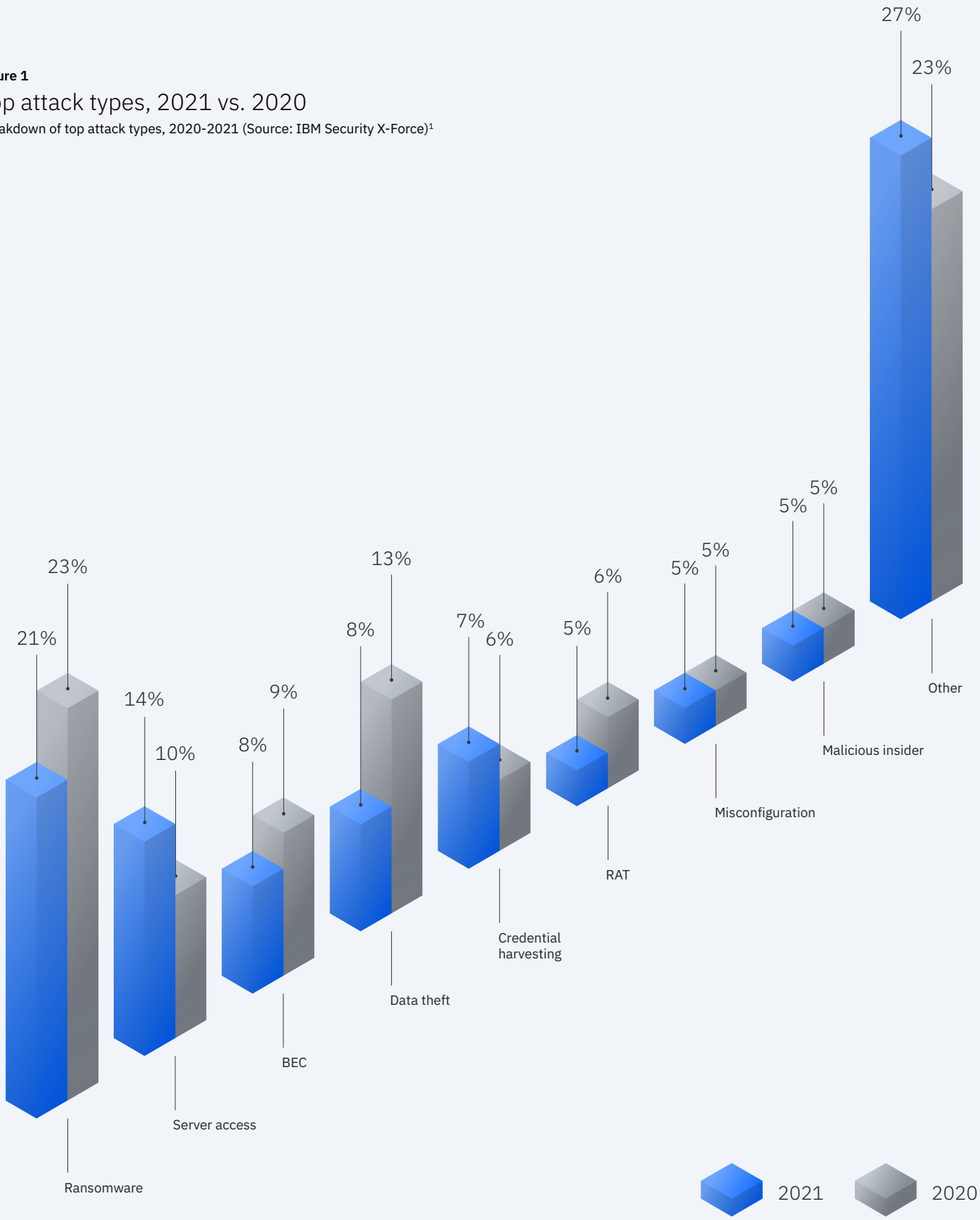
Ransomware

For more than three years, ransomware has been the top attack type observed by X-Force, and 2021 was no exception. Twenty-one percent of attacks remediated by X-Force incident response in 2021 were ransomware attacks. This is down slightly from the year prior, when 23% of attacks X-Force remediated were ransomware attacks; however, the volume of ransomware attacks has remained steady year-over-year.

Figure 1

Top attack types, 2021 vs. 2020

Breakdown of top attack types, 2020-2021 (Source: IBM Security X-Force)[1]



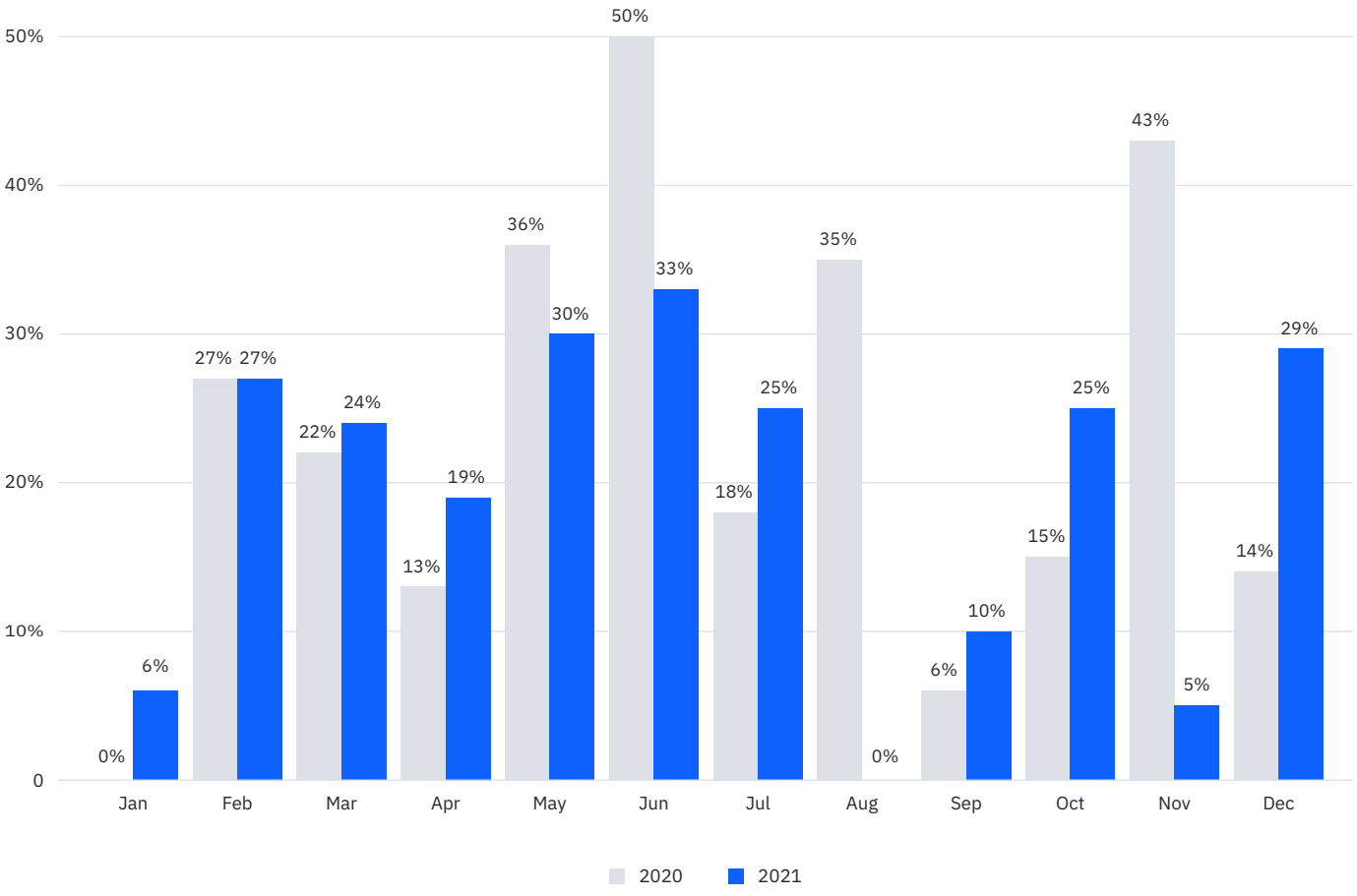
[1] Other attacks include adware, banking trojans, botnets, cryptominers, defacements, fraud, DDoS, point of sale malware, spam, webscripts, webshells, and worms.

The frequency of ransomware attacks X-Force observes tends to shift throughout the year, with May and June tending to see higher frequencies of attacks, while January tends to see lower. In addition, ransomware attacks appear to decrease in late summer or early fall. In 2021, that drop largely came in August and again in November, likely spurred by the permanent or temporary shutdown of several groups in the months prior: DarkSide and Babuk in May, Avaddon in June, and REvil in October.

Figure 2

Percentage of IR incidents that were ransomware, by month, 2020 vs. 2021

Percentage of X-Force Incident Response engagements that were ransomware, 2020-2021 (Source: IBM Security X-Force)



According to X-Force research, 17 months is the average time before a ransomware group either rebrands or shuts down, with a median of 18 months. Ransomware groups often spring up and rebrand once there is a threat of arrest or action by law enforcement. In some cases, law enforcement action forces ransomware groups to shut down entirely. Despite this dynamic environment—or perhaps because of it—many ransomware actors remain at large, and X-Force assesses that criminal ransomware activity will continue into the foreseeable future, based on the high profits generated by this activity and current limitations on law enforcement for widely shutting down ransomware activity. X-Force is aware of many ransomware actors that have rebranded and continued operations under new names, with GandCrab to REvil, Maze to Egregor, and DoppelPaymer to Grief as examples.

Law enforcement activity is probably the primary factor driving down the percentage of ransomware attacks X-Force observed in 2021, but it is very likely that the groups we have seen disappear will rebrand and re-emerge in 2022 under new names and that ransomware activity will continue.

> “Many ransomware actors have continued operations under new names”

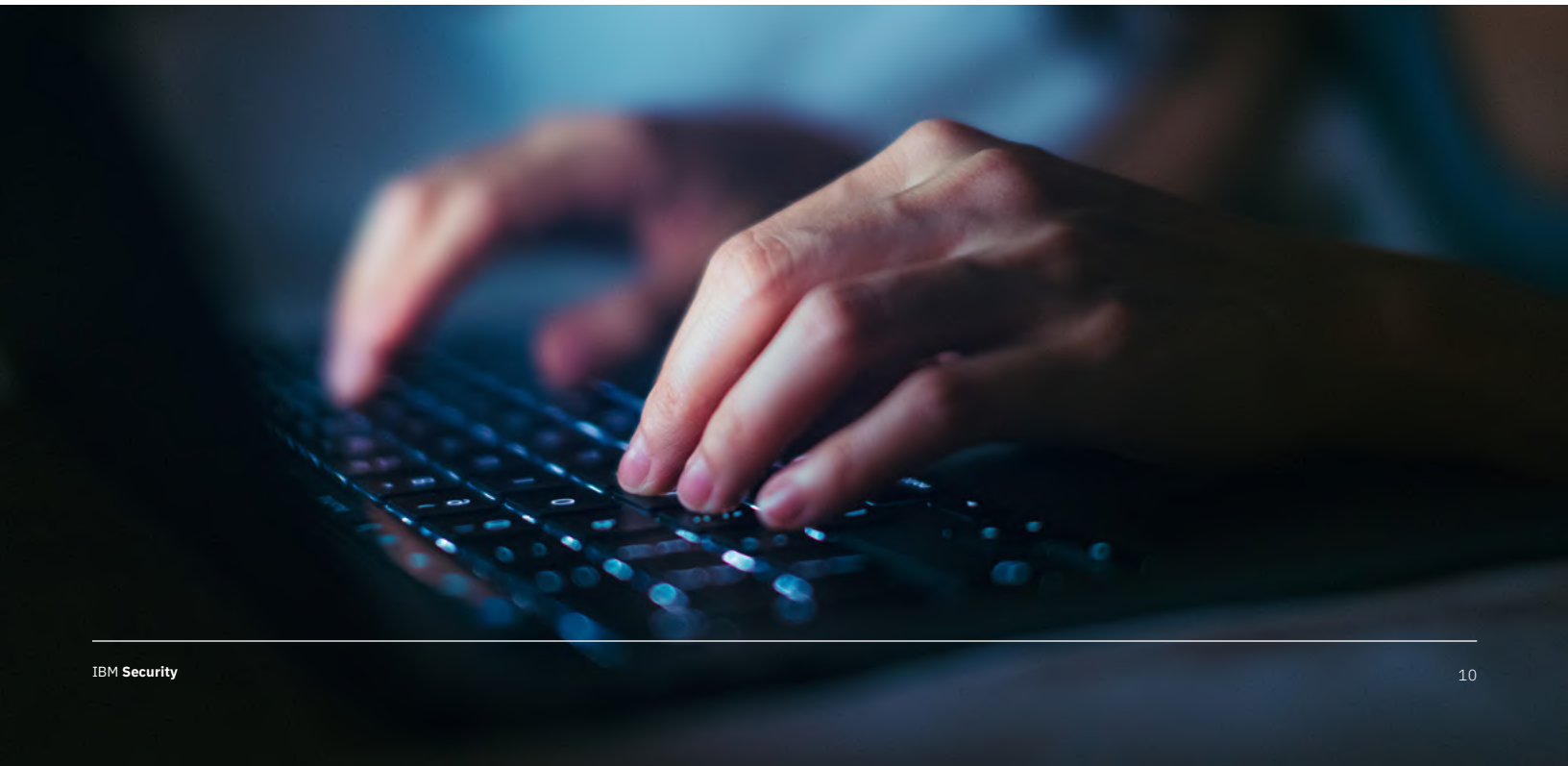
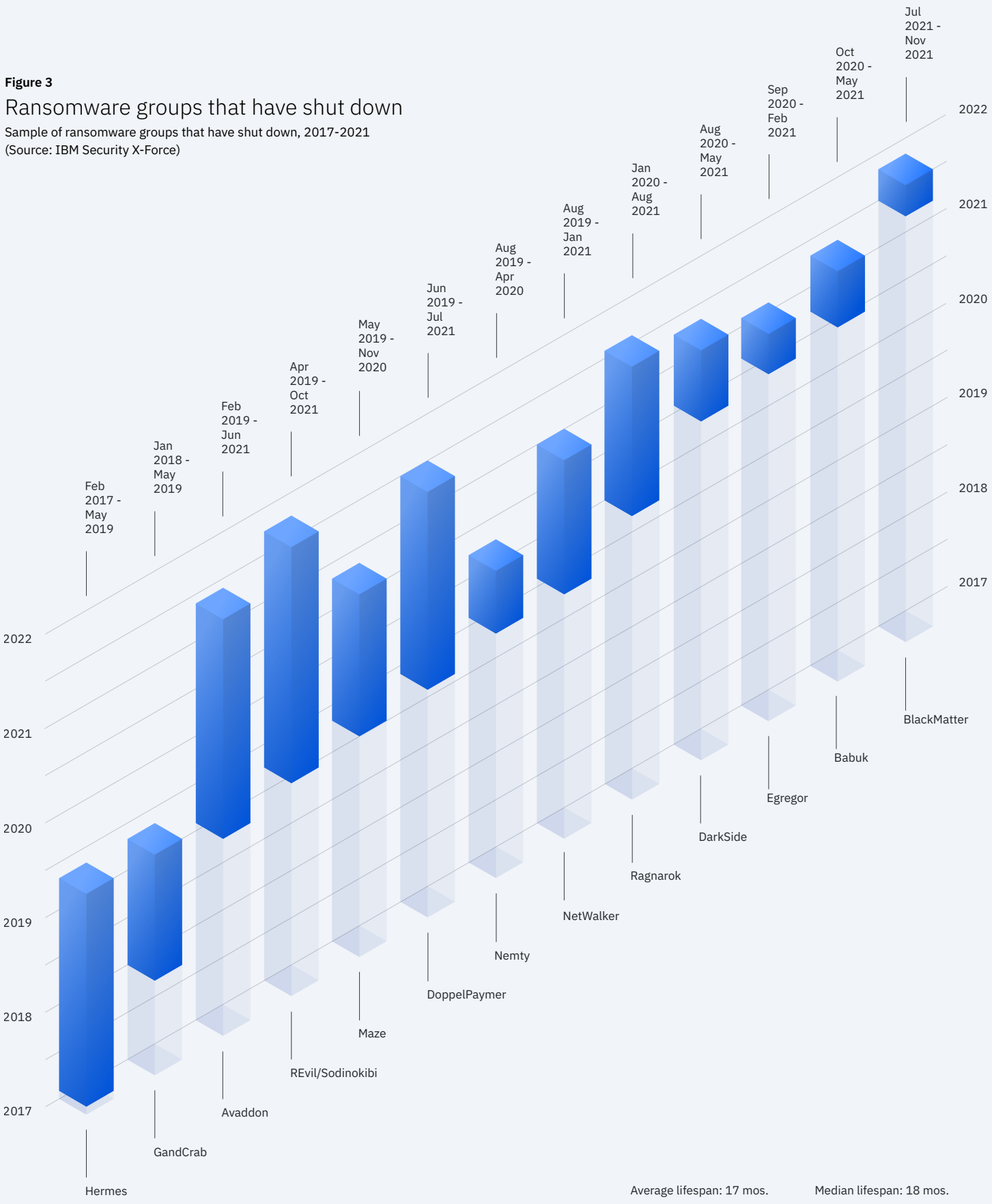


Figure 3

Ransomware groups that have shut down

Sample of ransomware groups that have shut down, 2017-2021
(Source: IBM Security X-Force)

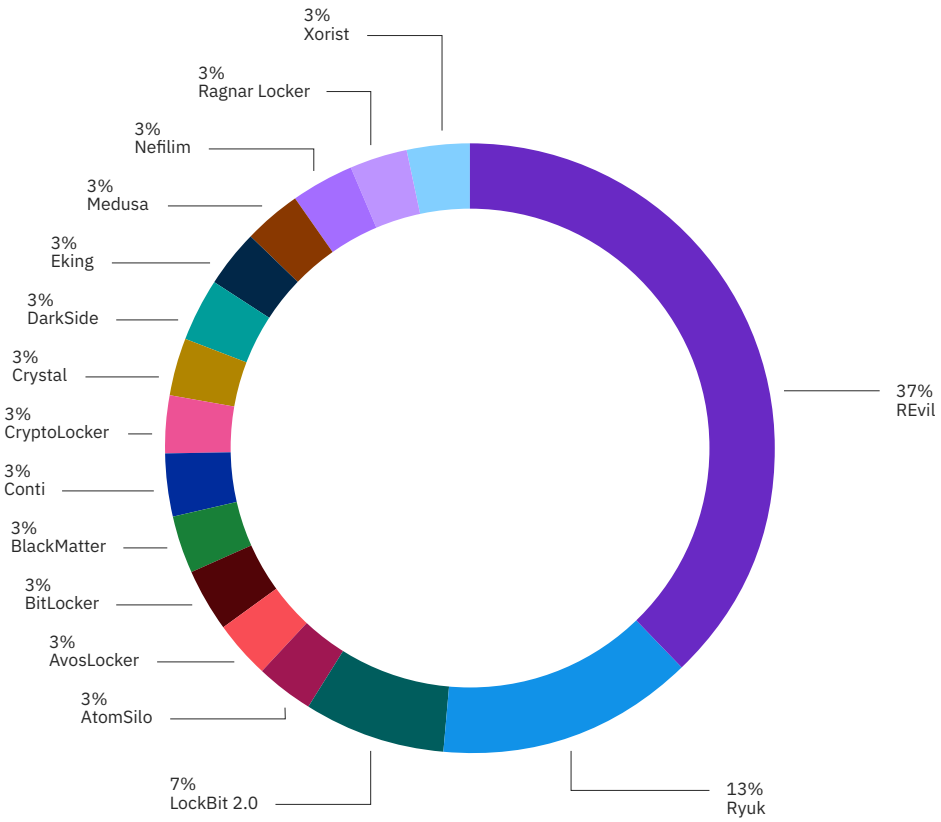


Of the ransomware strains observed by X-Force in 2021, REvil made up 37%—over one-third—of all ransomware incidents our team remediated. A strong second was Ryuk, making up 13% of attacks observed last year. REvil actors as of mid-October 2021 appear to have permanently shut down operations, probably due to law enforcement activity. Both Ryuk and REvil constitute some of the longest-running ransomware operations, having emerged in April 2019 and August 2018, respectively.

Figure 4

Types of ransomware observed in 2021

Ransomware types observed by X-Force Incident Response in 2021
(Source: IBM Security X-Force)



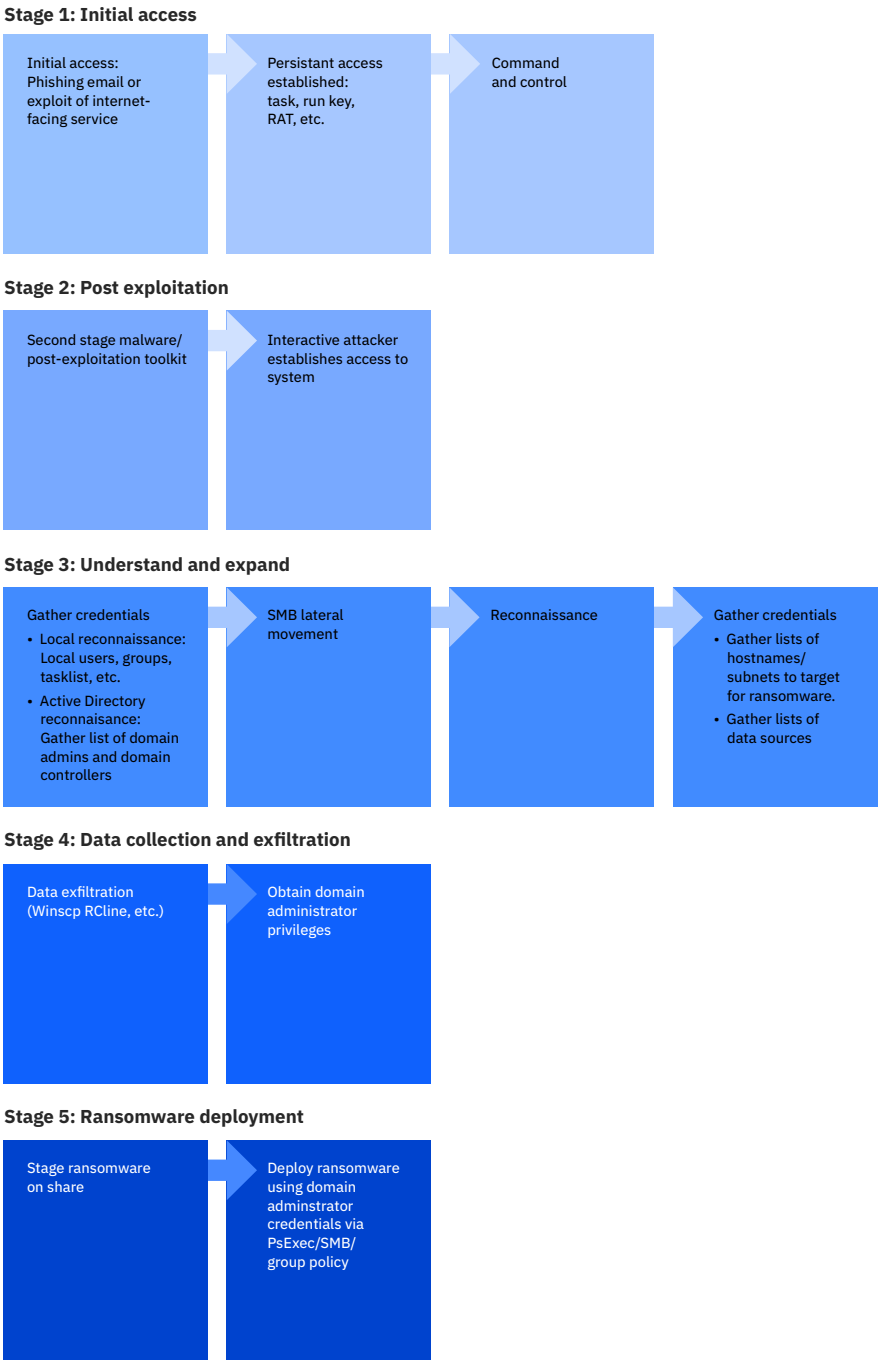
How ransomware attacks happen

Given the deep experience X-Force Incident Response (X-Force IR) has in remediating ransomware attacks, our team has observed a recent pattern emerge across the vast majority of ransomware attacks. In particular, we have been able to develop a five-stage model that defines the common pattern observed in most ransomware incidents.

Figure 5

Stages of a ransomware attack

Standard attack flow for ransomware attacks, as observed by X-Force Incident Response (Source: IBM Security X-Force)



Stage 1: Initial access

The most common access vectors for ransomware attacks continue to be phishing, vulnerability exploitation, and remote services such as remote desktop protocol.

Stage 2: Post exploitation

Depending on the initial access vector, the second stage may involve an intermediary remote access tool (RAT) or malware prior to establishing interactive access with an offensive security tool such as Cobalt Strike or Metasploit.

Stage 3: Understand and expand

During the third stage of the attack, attackers have consistently focused on understanding the local system and domain that they currently have access to and acquiring additional credentials to enable lateral movement.

Stage 4: Data collection and exfiltration

Almost every ransomware incident X-Force IR has responded to since 2019 has involved the “double extortion” tactic of data theft and ransomware. During stage 4 of the attack, the focus of the ransomware operators switched primarily to identifying valuable data and exfiltrating it.

Stage 5: Ransomware deployment

In almost every single ransomware incident X-Force IR has responded to, the ransomware operators targeted a domain controller as the distribution point for the ransomware payload.

A concerning new trend in ransomware has been the expansion of “triple extortion” tactics. In this type of attack, threat actors encrypt and steal data and also threaten to engage in a distributed denial of service (DDoS) attack against the affected organization. This kind of attack is particularly problematic for organizations because victims have their networks held hostage with two kinds of malicious attacks—often simultaneously—and are then further victimized by the theft (and often leak) of data.

Ransomware gangs are beginning to look to their primary victim’s extended business partners to pressure them into paying a ransom to prevent their own data leakages or business disruptions caused by the ransomware attack.

11%

of attacks were server access

Server access

Server access attacks—where the attacker gained unauthorized access to a server, but the final end goal is unknown—was the second-most common attack type, making up 11% of all incidents X-Force IR team remediated in 2021.

The majority of these attacks occurred in Asia, and in many cases the threat actors were successful in deploying malware or employing penetration testing tools on a server, including China Chopper Webshells, Black Orifice malware, Printspoofer, and Mimikatz.

In some instances, the threat actors exploited a known vulnerability, such as CVE-2020-7961, which would allow for remote code execution on a server. In multiple cases threat actors exploited vulnerabilities in Microsoft Exchange servers to gain unauthorized access to networks of interest. These vulnerabilities are included in the top 10 vulnerabilities of 2021 listed below.

Some of the server access attacks observed by X-Force’s IR team may have been failed attempts to steal data or deploy ransomware. Thus, while companies aim to prevent attackers from gaining any level of unauthorized access to their networks, it’s likely that a high number of server access attacks indicates that organizations are identifying and eradicating attacks before they progress into more damaging operations.

Business email compromise

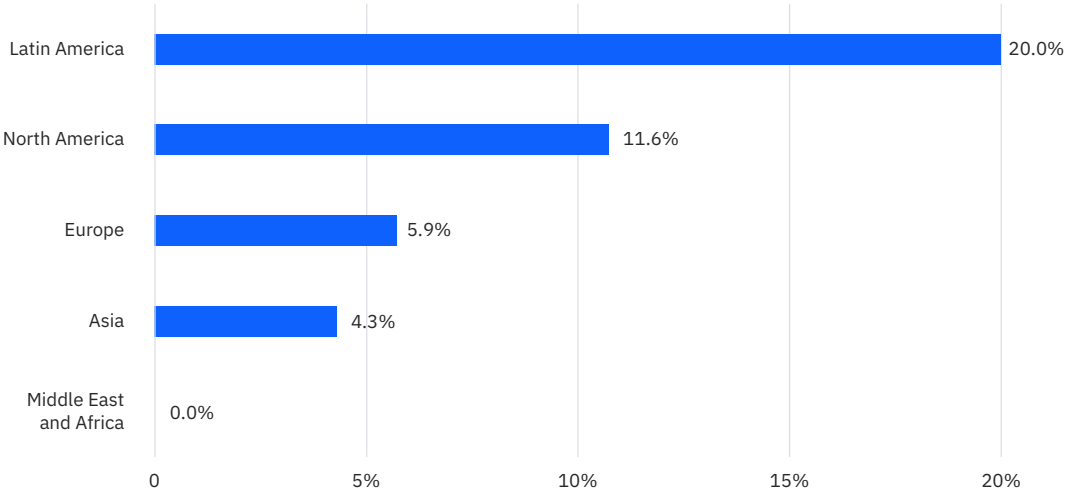
After a downturn in business email compromise (BEC) attacks in 2020, X-Force observed a decrease in this attack type again in 2021. BEC was the third-most common attack type remediated by our X-Force IR team. Last year, we theorized that widespread implementation of multifactor authentication (MFA) was decreasing the number of successful attacks BEC threat actors were able to execute. That theory held in 2021, since BEC attackers may have realized greater success by shifting focus to geographies where MFA is not as widely implemented.

For example, Latin American organizations appeared to be bearing the brunt of BEC attacks the X-Force IR team is remediating. North American organizations were still strongly in the crosshairs of BEC operations, but the surge we noticed against Latin American organizations suggests that BEC attackers shifted the geographic focus of their operations: zero percent of attacks against Latin American organizations were BEC in 2019, but 19% of attacks were BEC in 2020 and 20% of attacks in 2021 were BEC.

Figure 6

Percentage of incidents that were BEC, 2021

Percentage of incidents that were BEC in each region, 2021 (Source: IBM Security X-Force)



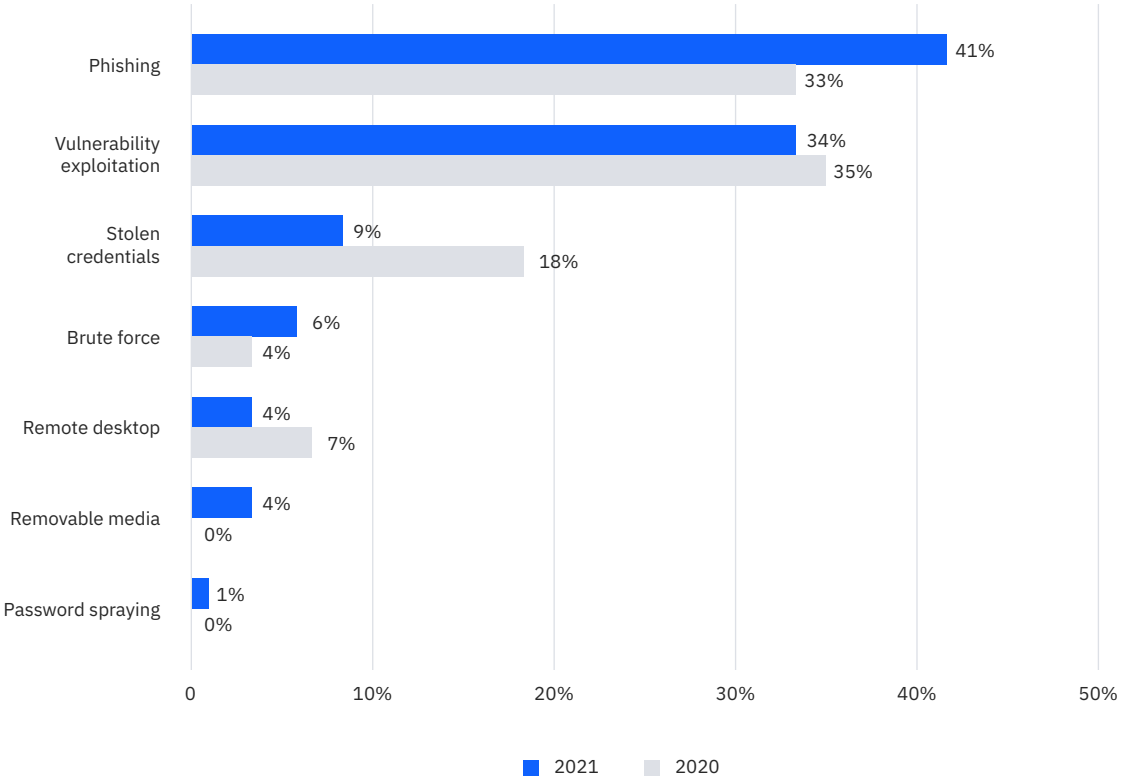
Top infection vectors

In addition to examining the end goal of threat actors X-Force observes, our team also tracks how threat actors gain initial access to victims' networks. Phishing and vulnerability exploitation tend to be the most common methods we observe, followed by use of stolen credentials, brute force, remote desktop protocol (RDP), removable media and password spraying making up a small percentage of intrusions.

Figure 7

Top infection vectors, 2021 vs. 2020

Breakdown of infection vectors observed by X-Force Incident Response, 2020-2021 (Source: IBM Security X-Force)



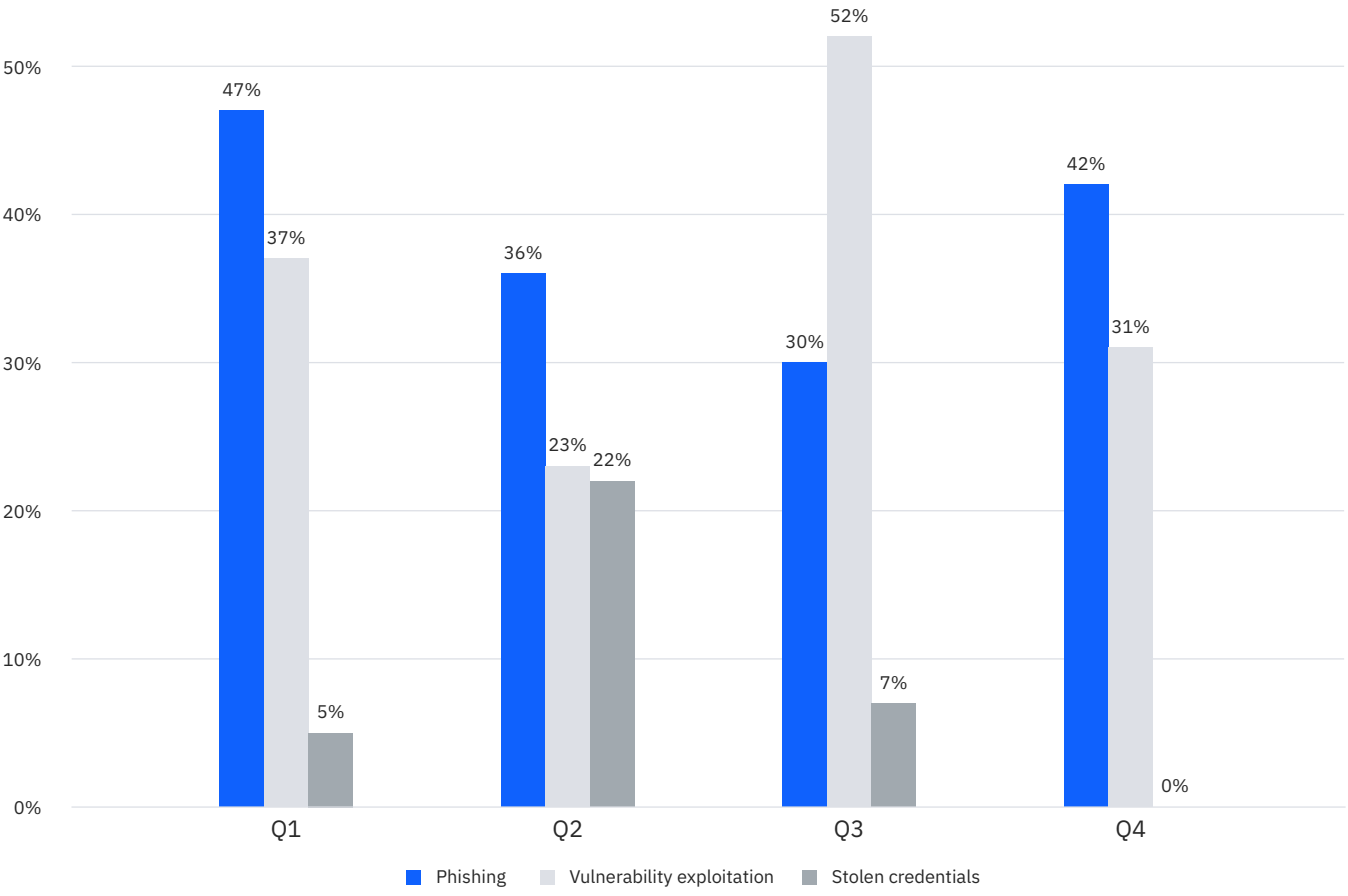
Phishing

Phishing emerged as the top infection vector in 2021, surpassing vulnerability exploitation, which took the lead in 2020. Phishing was observed in 41% of the incidents X-Force remediated. While vulnerability exploitation dominated in Q3 of 2021, the significant number of phishing-related incidents X-Force observed in Q1 and Q4 pushed this infection vector into the lead for the year.

Figure 8

Percentage of attacks tied to phishing, vulnerability exploitation, and stolen credentials, by quarter, 2021

Percentage of attacks linked with various infection vectors, by quarter, in 2021 (Source: IBM Security X-Force)



Part of X-Force Red's focus areas include conducting social engineering penetration testing attacks through phishing emails. For targeted phishing campaigns in 2020 and 2021, the average click rate for an X-Force Red simulated campaign was 17.8%. When vishing (voice phishing) phone calls were added to the campaign, the click rate rose to 53.2%, three times as effective.

BEC attackers have leveraged phishing campaigns and social engineering with great success. And particularly in 2021, X-Force observed ransomware actors rely even more heavily on phishing campaigns to gain initial access to victim networks for ransomware attacks.

For example, multiple REvil ransomware incidents observed in 2021 began with a QakBot phishing email. These emails usually have very short messages, often refer to unpaid invoices, and occasionally will even hijack ongoing email conversations and reply all with only a malicious attachment.

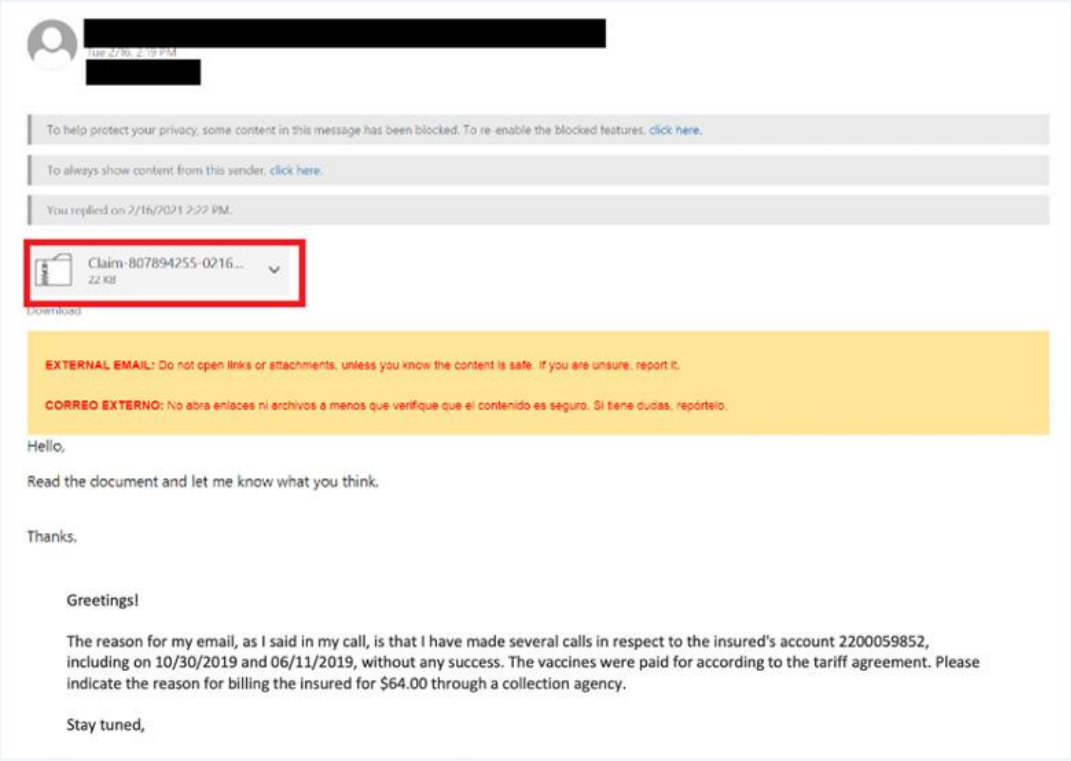
When opened, the document will instruct the recipient to enable macros which will drop the QakBot banking trojan, gaining an initial foothold on a system. The operation is then transferred to REvil ransomware actors who conduct reconnaissance and proceed with the operation from there.

A sample QakBot phishing email is included in figure 9.

Figure 9

Sample QakBot phishing email

Example of QakBot phishing email with malicious attachment (Source: IBM Security X-Force)

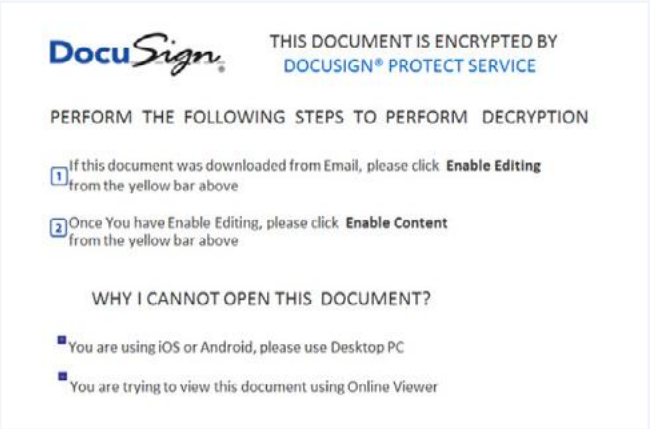


When the recipient attempts to open the attachment, they are prompted by a popup (see figure 10) to enable macros by choosing “Enable editing” and “Enable content.” This allows the threat actor to deploy malware on the victim’s machine with the assistance of malicious macros.

Figure 10

Sample popup message from QakBot phishing attachment

Message in malicious attachment prompting the recipient to enable macros (Source: IBM Security X-Force)



Phishing kit deployments short-lived, abuse technology and bank brands

IBM analyzed thousands of phishing kits from around the world to determine the frequency and effectiveness of this particular attack vector. Our investigation suggests that malicious actors who use phishing kits probably put in tedious hours with limited gains. In particular, our investigation showed that:

— Phishing kit deployments generally had a short lifespan, with almost one-third of deployed kits being used for no longer than a day. In some cases, an individual deployment of a phishing kit lasted only seven-to-eight hours before most hosting providers identified the site as malicious and blocked it.

— Each deployment on average had no greater than 75 potential victims who visited the site.

— Phishing kits asked for user credentials (email/ID/password combinations) in nearly every kit observed (close to 100%), followed in popularity by credit card data (61% of requests), mailing address (40%), phone number (22%), date of birth (17%), identity card number (15%), security questions (14%), and ATM PINs (3%).

In addition, X-Force looked at which brands were most frequently spoofed in phishing kits. The top brands included large technology companies and large financial institutions. The top 11 brands are listed below.

Top 11 most spoofed brands of 2021

1. Microsoft
2. Apple
3. Google
4. BMO Harris Bank (BMO)
5. Chase
6. Amazon
7. Dropbox
8. DHL
9. CNN
10. Hotmail
11. Facebook

222,127

phishing attacks in June 2021, setting an all-time record high

The Anti Phishing Work Group (APWG) noted that June 2021 set an all-time record high with 222,127 phishing attacks that month alone. X-Force assesses with high confidence that phishing kits will continue to be used by threat actors due to their easy-to-use nature and low resource requirement. Monitoring for suspicious connections to likely spoofed brands can help organizations minimize the probability of impact from this attack vector.

Using a DNS service that's dedicated to data privacy, like Quad9[2], can also help mitigate the risk of phishing attacks.

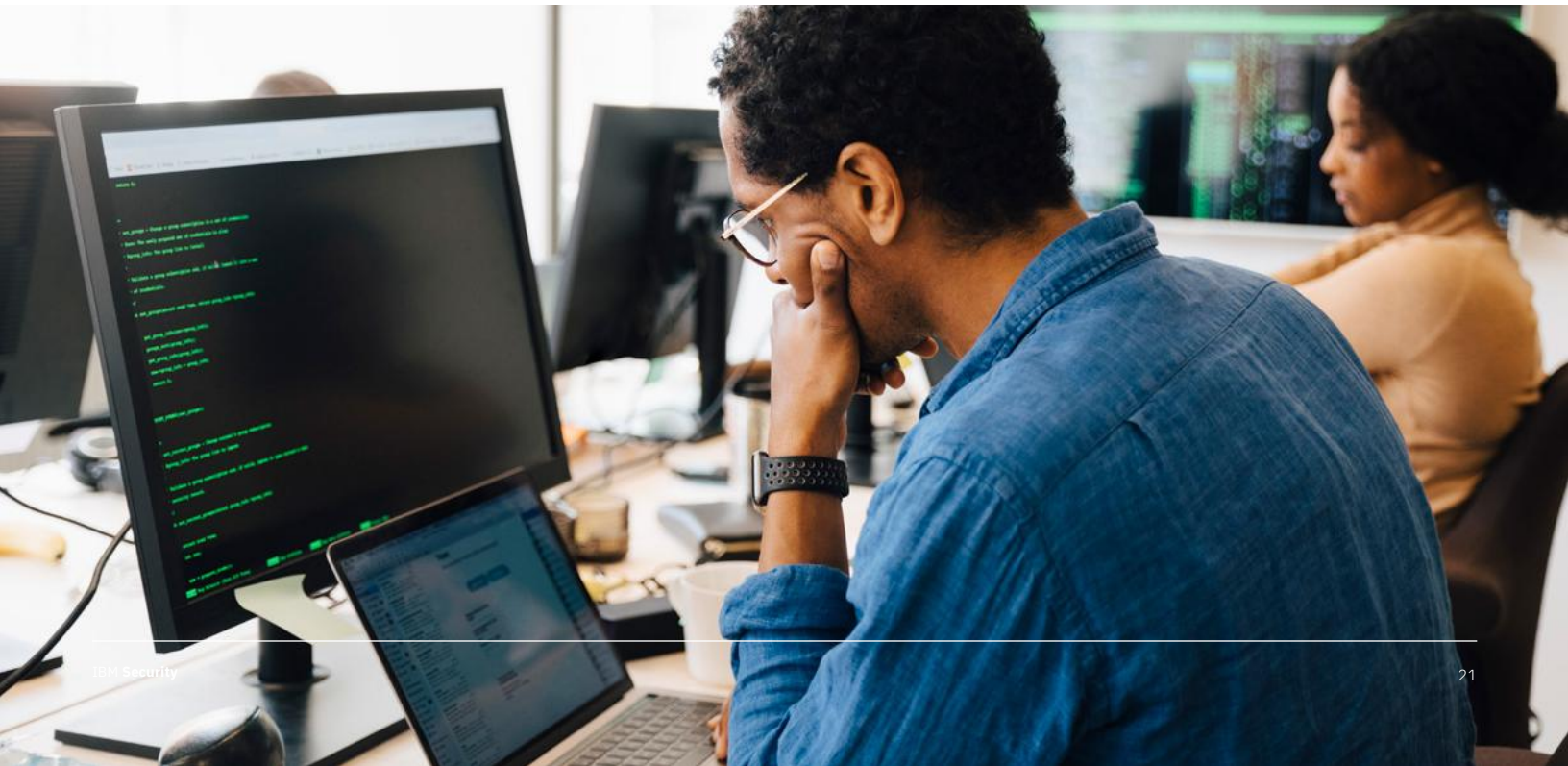
[2] IBM Security X-Force is a Quad9 partner.

Vulnerability exploitation

Despite dropping to the second-most common in 2021, the number of incidents that were caused by vulnerability exploitation this past year rose 33% from 2020, indicating this attack vector's strong hold in threat actors' arsenals. This vector allows threat actors to gain access to victim networks for further operations—in many cases with elevated privileges.

X-Force observed actors leveraging multiple known vulnerabilities, such as CVE-2021-35464 (a Java deserialization vulnerability) and CVE-2019-19781 (a Citrix path traversal flaw), to gain initial access to networks of interest. In addition, we observed threat actors leverage zero-day vulnerabilities in major attacks like the Kaseya ransomware attack and Microsoft Exchange Server incidents to access victim networks and devices.

Near the end of 2021, widespread exploitation of the Log4j vulnerability CVE-2021-44228 also launched this vulnerability into second place in X-Force's top 10 list for 2021. Several mitigation measures can assist your organization in avoiding becoming a victim of this vulnerability.



Number of vulnerabilities hit another record high

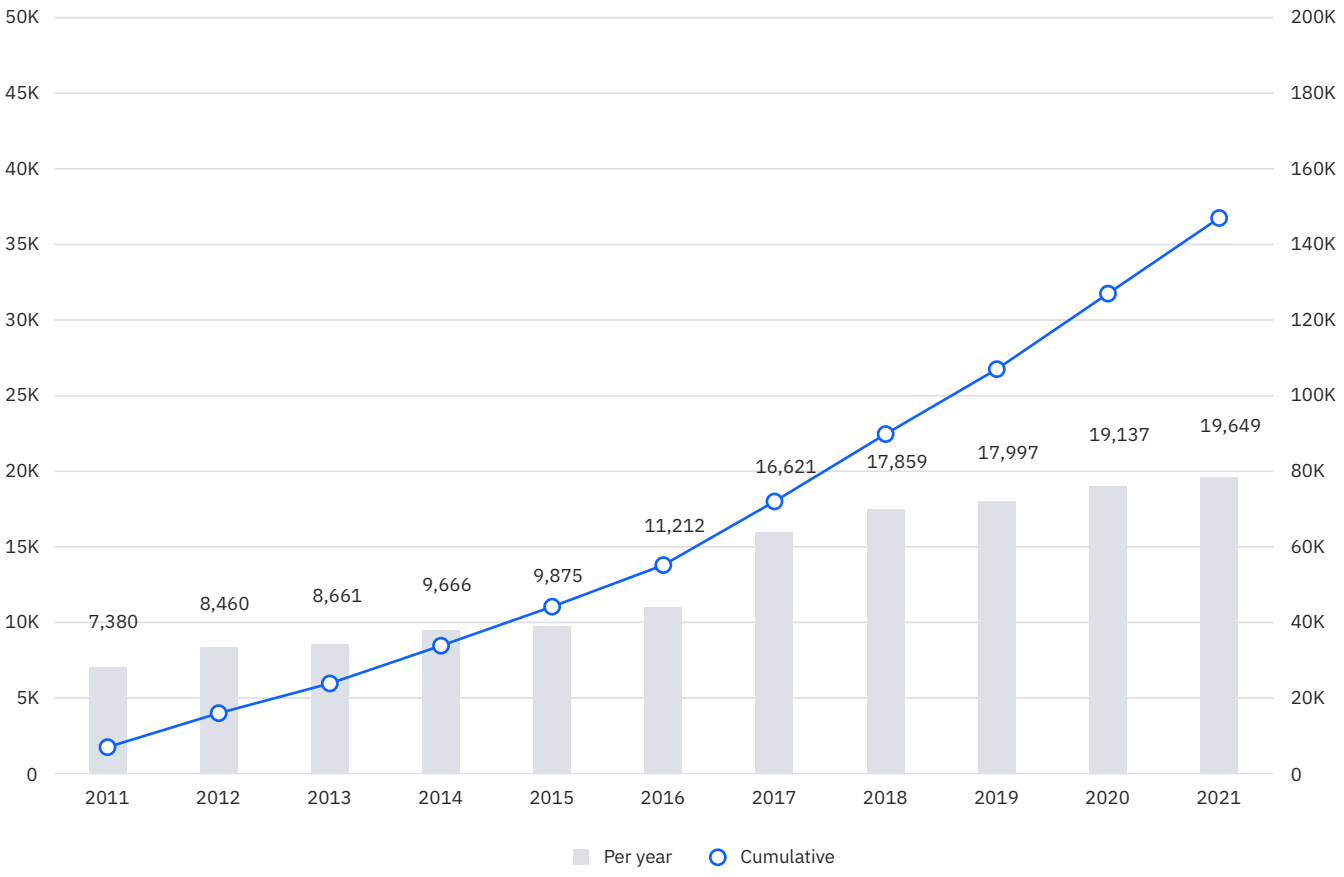
Over the past five years, the number of vulnerabilities discovered per year his risen steadily. Even more concerning is that the number of exploits—tools threat actors can use to exploit a vulnerability—are also rising steadily, creating an ever-expanding array of options for threat actors seeking to exploit vulnerabilities.

Vulnerabilities related to Internet of Things (IoT) and industrial control systems (ICS) increased at an even faster rate than overall vulnerabilities, with these two categories experiencing a 16% and 50% year-over-year increase respectively, compared to a 0.4% growth rate in the number of vulnerabilities overall.

Figure 11

Vulnerabilities discovered by year, 2011-2021

New vulnerabilities identified each year, 2011-2021, and cumulative number of vulnerabilities (Source: IBM Security X-Force)



Top 10 vulnerabilities of 2021

While any vulnerability carries risk and should be assessed, the following list includes the top vulnerabilities that X-Force IR observed threat actors exploit or attempt to exploit during the course of operations in 2021. X-Force recommends prioritizing patching of these vulnerabilities if your organization has not done so already.

1. CVE-2021-34523 – Microsoft Exchange server flaw enabling malicious actors to bypass authentication and impersonate an administrator. Known generically as ProxyLogon.
2. CVE-2021-44228 – Vulnerability in Apache Log4j Library
3. CVE-2021-26857 – Microsoft Exchange Server remote code execution vulnerability
4. CVE-2020-1472 – Netlogon elevation of privilege vulnerability
5. CVE-2021-27101 – Accellion FTA vulnerability susceptible to SQL injection
6. CVE-2020-7961 – Liferay Portal deserialization of untrusted data allows for remote code execution via JSON web services
7. CVE-2020-15505 – MobileIron vulnerability allowing for remote code execution
8. CVE-2018-20062 – NoneCMS ThinkPHP remote code execution vulnerability
9. CVE-2021-35464 – ForgeRock AM server Java deserialization vulnerability allows for remote code execution
10. CVE-2019-19781 – Citrix Server path traversal flaw

Threats to operational technology and Internet of Things

Known vulnerabilities related to industrial control systems (ICS)—and, by extension, operational technology (OT)—as well as Internet of Things (IoT) vulnerabilities are increasing each year, with an appreciable increase in identified vulnerabilities from 2020 to 2021.

As more "things" come alive with the power of digitization and internet protocols, so do new vulnerabilities and risks. While many of these issues affect only industrial organizations, any organization that uses IoT in its infrastructure is also increasingly exposed to risk.

In addition to this increased digitization, the dynamics of supply chains are affecting the attack surface for many OT-connected organizations. Threat actors understand the critical role manufacturing and energy play in global supply chains and are seeking to disrupt these organizations because of the ripple effect it can have across multiple industries and the pressure these multiplying effects create for victims to pay a ransom.

Threat actors accelerate reconnaissance against OT devices

Analyzing data from 2021, X-Force observed attackers conducting massive reconnaissance campaigns searching for exploitable communications in industrial networks. Specifically, 2021 saw a considerable increase in reconnaissance activity targeting TCP port 502.

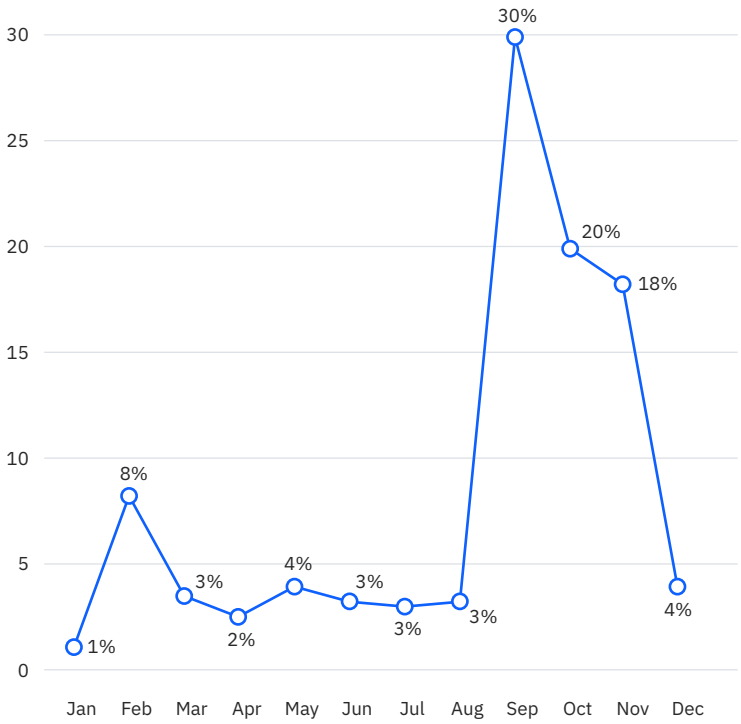
This port uses Modbus, an application layer messaging protocol used to provide client-to-server communication between connected buses, networks, and programmable logic controller (PLC) devices in industrial networks. Port 502 is commonly used by supervisory control and data acquisition (SCADA). Access to Modbus could allow threat actors to control physical devices connected to the internet.

Between January and September of 2021, X-Force observed a 2204% increase in adversarial reconnaissance activity targeting port 502.

Figure 12

SCADA Modbus reconnaissance volume, breakdown by month, 2021

Month-by-month breakdown of SCADA Modbus reconnaissance activity, 2021 (Source: IBM Security X-Force)



Threat actors may have heightened Modbus reconnaissance to begin finding targets to ransom or seize control and cause harm. Given Modbus's lack of security features, once an attacker has found an accessible Modbus device, they could then issue harmful commands to the device and impact connected ICS or IoT systems.

Although SCADA Modbus resides in Level 2 of the Purdue Model within ICS environments—which ideally should be segmented from the enterprise network and placed behind a demilitarized zone—in some cases the SCADA Modbus port 502 can be accessed directly over the open internet. Lack of authentication and transmission of messages in plain text are some additional aspects of Modbus that make it less secure when compared to other, more modern technologies.

Manufacturing most targeted of OT industries, ransomware leads

In terms of industries with OT networks, X-Force observed manufacturing was the most attacked in 2021 by a significant margin, victimized in 61% of incidents X-Force assisted in remediating. Ransomware actors in particular find manufacturing to be an attractive target, likely due to these organizations' low tolerance for down time.

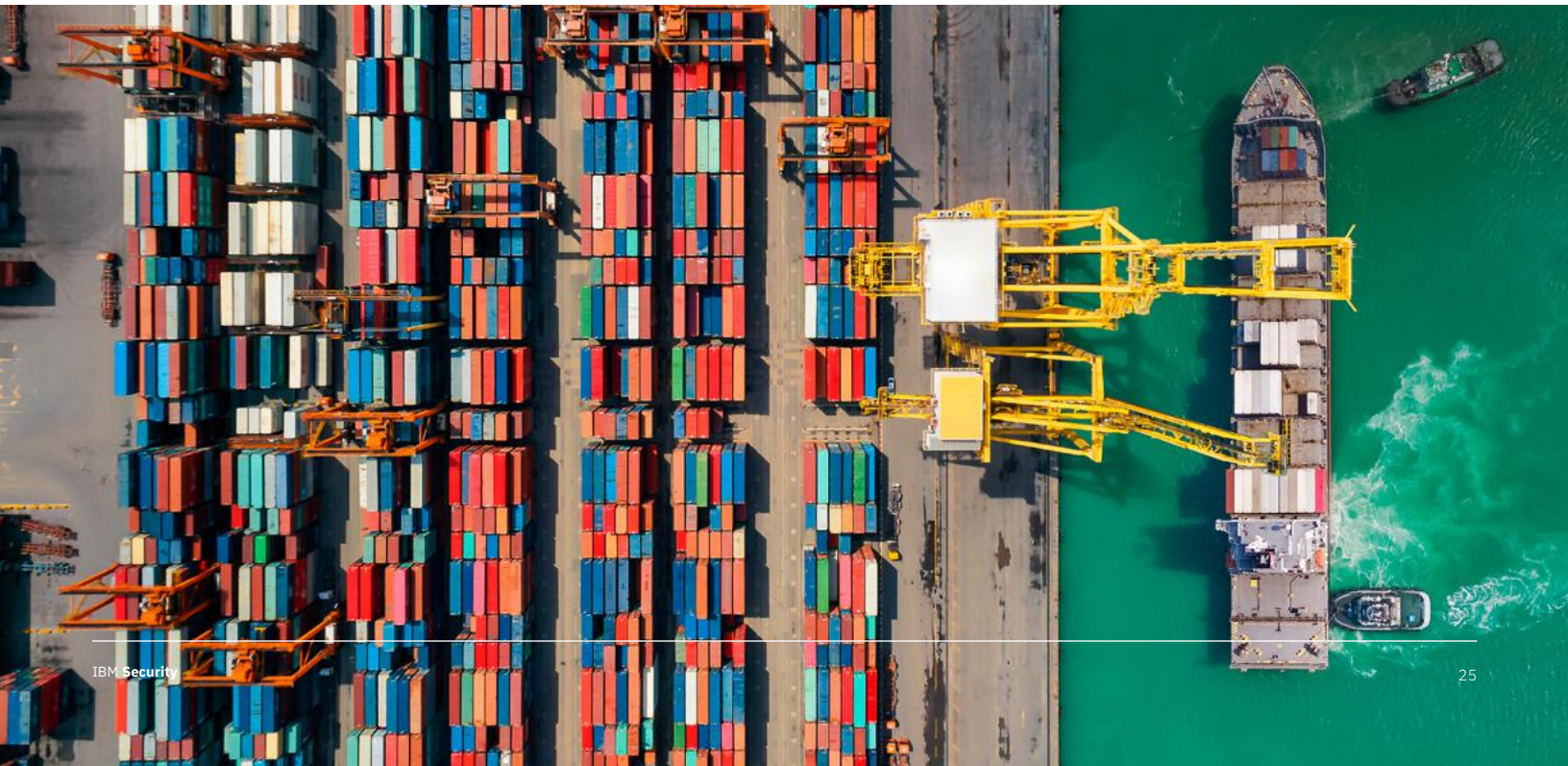


Figure 13

OT industries targeted, 2021

Breakdown of attacks against six operational technology industries targeted, as observed by X-Force IR, 2021 (Source: IBM Security X-Force)

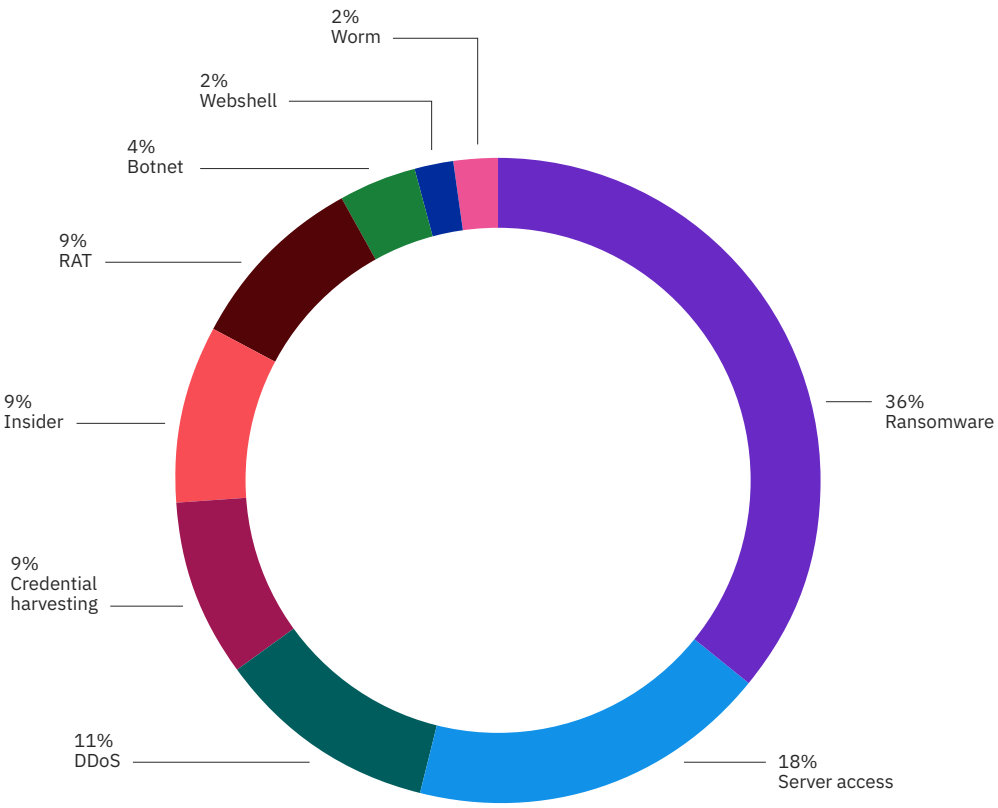
For all industries with OT networks where X-Force observed attacks in 2021—engineering, mining, utilities, oil and gas, transportation and manufacturing—ransomware again led the charge for attack types, accounting for 36% of all attacks and echoing the overall attack trend across all industries. While the IT networks were compromised in the vast majority of these attacks, the impact carried over to victims' operational technology in many of these instances.

Other top attack types included server access, DDoS, RATs, insiders, and credential harvesting operations.

Figure 14

Attack types on OT, 2021

Breakdown of attack types on operational technology, 2021
(Source: IBM Security X-Force)



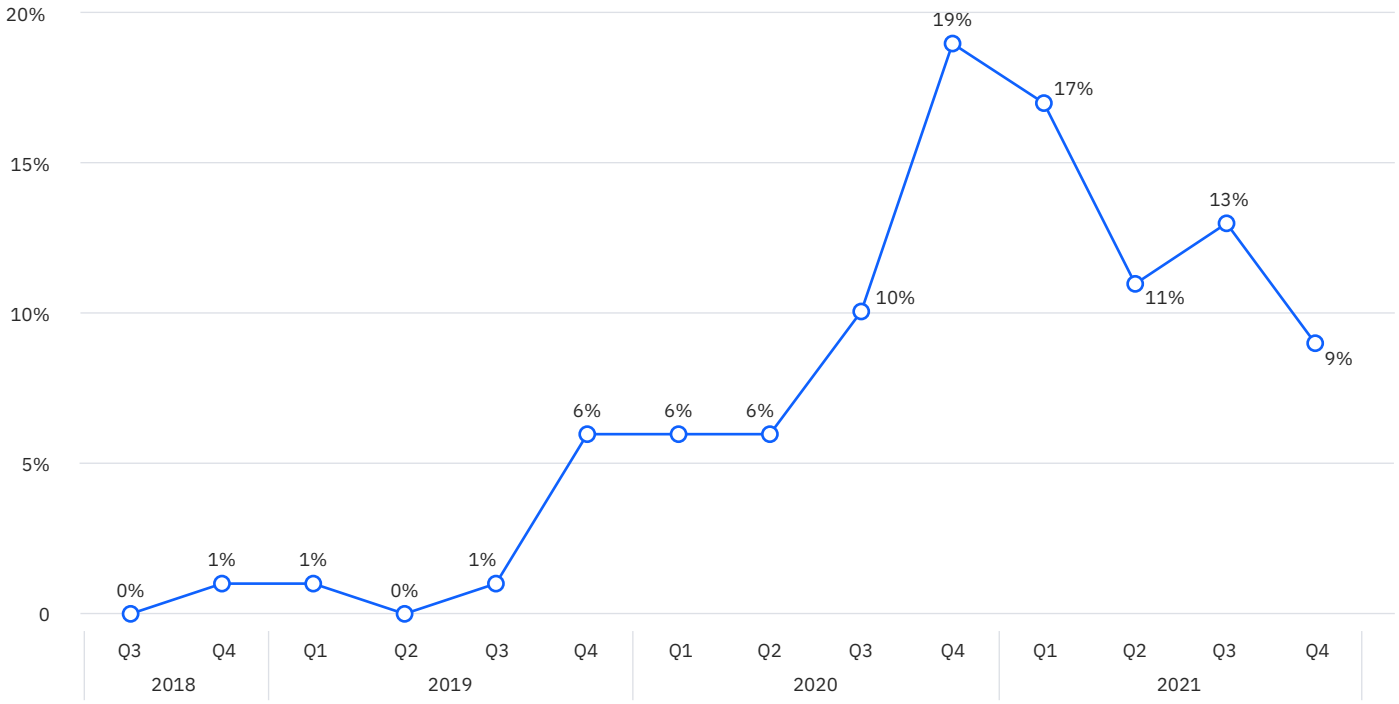
Mozi botnet continues to threaten IoT and OT assets

Since 2019, X-Force has identified a high volume of IoT malware activity—including a nearly 3000% surge between Q3 2019 and Q4 2020. The Mozi botnet continued to make up the most significant volume of IoT malware compared to all other IoT malware types, at 74% of the total volume of IoT malware X-Force observed in 2021.

Figure 15

IoT attack volume breakdown by quarter, 2018-2021

IoT malware activity, broken down by quarter, 2018-2021 (Source: IBM Security X-Force)



Mozi abuses weak Telnet passwords and exploits vulnerabilities to target networking devices, IoT, and video recorders, among other internet-connected products. Post-infection, it is capable of maintaining persistence on network gateways, which can be particularly effective initial access points for lateral movement to high-value networks, including OT and ICS networks. In addition, by infecting routers, threat actors behind Mozi can position themselves to conduct man-in-the-middle attacks that lead to ransomware deployment, including attacks on OT networks.

In addition to Mozi's access and lateral movement capabilities, a large Mozi botnet that infects a large number of security cameras or similar IoT devices at an organization can diminish an organization's ability to effectively conduct physical security operations.

Chinese law enforcement reportedly arrested the authors of the Mozi botnet in June and August 2021, and the decrease in IoT attack volume in Q4 2021 is probably a side-effect of these arrests.

Top threat actors of 2021

Our 2021 IR data show that where a threat actor could be identified, cybercriminals were the leading source of attacks.

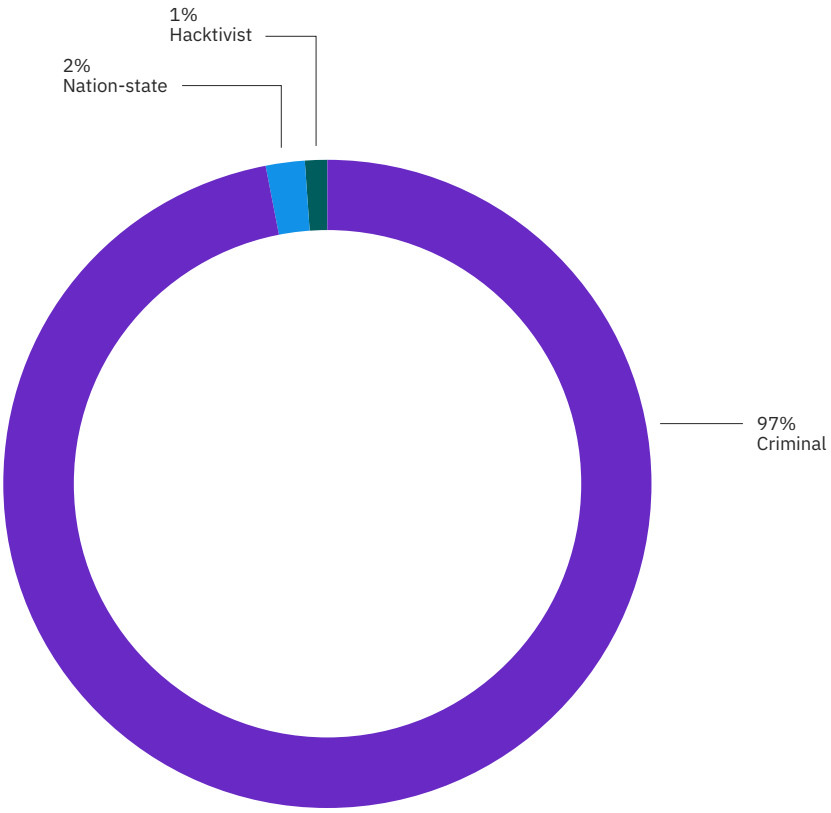
Nation-state actors made up only 2% of the engagements X-Force remediated in 2021, underscoring the high volume of activity generated by cybercriminal activity. The nation-state actors we observed were largely seeking to conduct espionage and surveillance, and in some cases, may have been laying the groundwork for future sabotage. Only 1% of the activity we observed was from hacktivist groups.

The following sections provide additional detail on some of the more interesting and active threat groups X-Force observed in 2021.

Figure 16

Threat actors observed by X-Force Incident Response, 2021

Threat actor groups observed by X-Force IR, broken down by type, 2021 (Source: IBM Security X-Force)



Suspected Iran-based ITG17 uses Aclip backdoor

In 2021, IBM Security X-Force observed a threat actor using a new backdoor that X-Force named "Aclip." In addition, the adversary leveraged a legitimate messaging and collaboration application tool likely to obfuscate operational communications, allowing malicious traffic, or traffic with underlying malicious intent, to go unnoticed. Based on the tools, tactics, and infrastructure observed, we assess with moderate confidence that the threat actor we track as ITG17[3] (aka MuddyWater), a suspected Iranian nation-state group, was behind this activity for the possible purpose of surveillance.

ITG23—Trickbot Gang—enables Conti ransomware operations

X-Force analysts have been closely tracking the cybercriminal group behind the Trickbot banking trojan—a group we identify as ITG23, also known as Wizard Spider or Trickbot Gang. Phishing emails with the Trickbot trojan are often used as an entry point for Conti ransomware, and X-Force has observed that an uptick in ITG23 Trickbot activity coincided with an uptick in Conti ransomware attacks.

The group has relied on email campaigns delivering malicious Excel documents, as well as the notable BazarCall campaign, in which subscription themed emails encourage recipients to contact a fraudulent call center where the telephone operator then guides the user to download the BazarLoader malware, under the guise of unsubscribing from a service. Additionally, the group has more recently been hijacking email threads and will then "reply all" with malicious attachments.

Hive0109 active in 2021

X-Force observed multiple Hive0109—also known as LemonDuck—compromises in 2021, and the group has proven itself adept at leveraging the ProxyLogon vulnerabilities to compromise unpatched Microsoft Exchange servers. LemonDuck targets both Linux and Windows systems and is known to capitalize on news-worthy events for phishing lures in its campaigns.

LemonDuck is persistent malware that was primarily used to mine cryptocurrency. It has likely been active at least since 2018 and has since evolved into a large botnet. LemonDuck propagates quickly and acts as a first-stage loader for subsequent malware and attacks. It continues to mine for crypto coins on infected devices.

[3] ITG stands for IBM Threat Group. This is IBM X-Force's naming convention for threat actor groups—both nation-state and cybercriminal. IBM tracks and names threat groups numerically, identified by IBM Threat Group (ITG) followed by an assigned number. For threat groups still in the research phase, we use the designation Hive, as in Hive0109 discussed in this section.

Trends in malware development

Threat actors continue to innovate and find new ways to make malware more capable across operating systems and more challenging to detect. This section describes some of the trends in malware development X-Force observed in 2021.

Next-level detection evasion

X-Force's malware reverse-engineering team uncovered over the last year significant upgrades in malware evasion techniques.

- Ransomware authors were employing different encryption techniques to avoid host-based detection systems. One example is intermittent encryption, where separated blocks of data are encrypted rather than the entire system, which speeds the encryption process.
- Command and control (C2) communications were increasingly using popular cloud messaging and storage services to blend into legitimate traffic. Additionally, the use of DNS for tunneling C2 communications was also becoming more prevalent. These techniques help attackers mask C2 activity from network-based sensors by posing as legitimate communications.
- Malware authors were utilizing increasingly sophisticated packing and code obfuscation techniques to hide the true purpose of the malware and hinder analysis attempts. Malware developers also experimented with different programming languages such as PureBasic and Nim to decrease the ease of reverse engineering.

Malware focus on Docker

Analyzing malware trends impacting cloud environments, X-Force IR observed multiple malware families shifting their sights from targeting generic Linux systems to focusing on Docker containers, often used in platform-as-a-service cloud solutions.

Some malware families illustrating this shift include XorDDoS, Groundhog and Tsunami. This Docker-focused push expands beyond just bots, also highlighting the malicious activity of IoT malware (Kaiji), cryptominers (Xanthe, Kinsing) and other malware strains that aim to leverage the power of cloud computing to scale their mining power.

Threat actors have also been observed targeting other container platforms in addition to Docker. For example, the Siloscape malware was found compromising vulnerable Windows containers and the Kubernetes container management platform. Siloscape is increasingly incorporated into attacks by actors such as TeamTNT, a cybercrime gang that's been focusing on cloud platforms to expand the reach of its cryptojacking botnets.

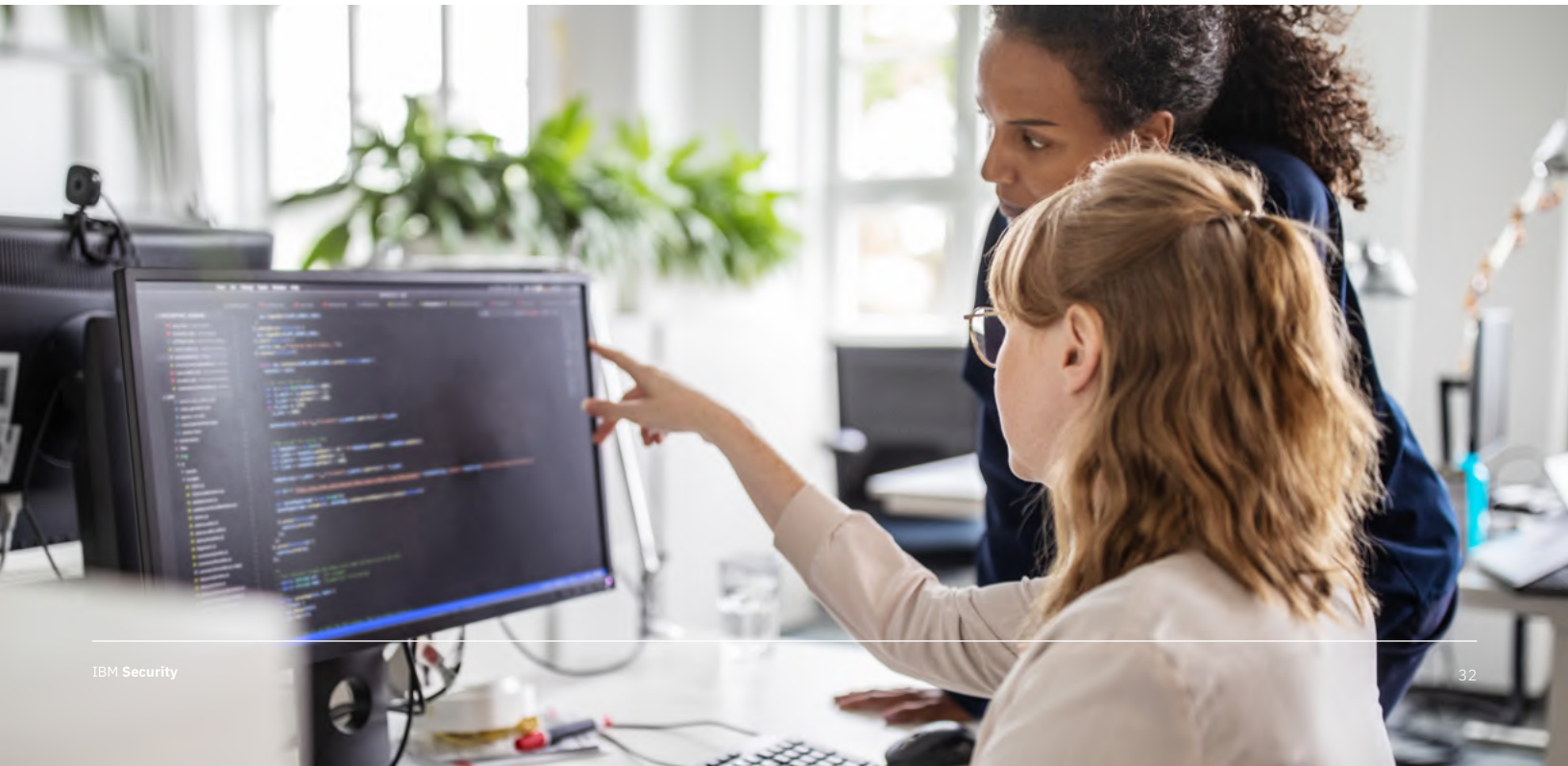
Ransomware focus on ESXi

Analyzing malware trends impacting Linux environments, X-Force observed multiple ransomware families shifting their sights to target Linux-based VMWare ESXi servers. As more organizations increasingly rely on virtualization, ransomware authors are discovering that it can be more effective to encrypt the virtual machine (VM) files themselves, rather than infecting the operating systems running within them.

In 2020, X-Force IR observed a Linux variant of the SFile ransomware deployed against an ESXi server, and in 2021 a number of other ransomware families appeared to follow suit, including REvil, HelloKitty, Babuk, and BlackMatter. These variants will often make use of ESXi's own command line management tool esxcli to enumerate and shut down running VMs before encrypting them.

Nim is in

In 2020, cross-platform malware developers gravitated to Golang as a programming language of choice, since it could be compiled for multiple operating systems at once. While Golang is still in use in 2021, additional languages such as Nim are becoming more popular. For example, threat actors used Nim to compile the Nimar backdoor as well as a version of Zebrocy—a malware type used by Russian nation-state actor ITG05 (aka APT28).



Linux threats continue to evolve

Analysis by IBM Security X-Force Threat Intelligence partner Intezer found that over the last year, malware targeting Linux environments dramatically increased, indicating continued threat actor interest in this space.

Intezer analyzes code uniqueness of malware strains to measure innovation. Malware code with more unique variations indicates more innovation has been used to edit the malware, whereas malware with mostly recycled code has less innovation. Using this methodology, the following results were reported.

Linux malware saw unique code increase in four out of five categories since the previous year, with the greatest increase being observed in banking trojans, which saw innovation increase over tenfold. This increase in Linux targeting may be correlated to organizations increasingly moving into cloud environments, which frequently rely on Linux for their operation.

The level of innovation of Linux malware came close to that of Windows-based malware, highlighting just how prevalent Linux malware innovation has become, a trend that we are sure to see increasing in 2022 as well.

Figure 17

Linux malware with unique code, 2021 vs. 2020

Linux malware with unique code in five categories, 2020-2021 (Source: Intezer)

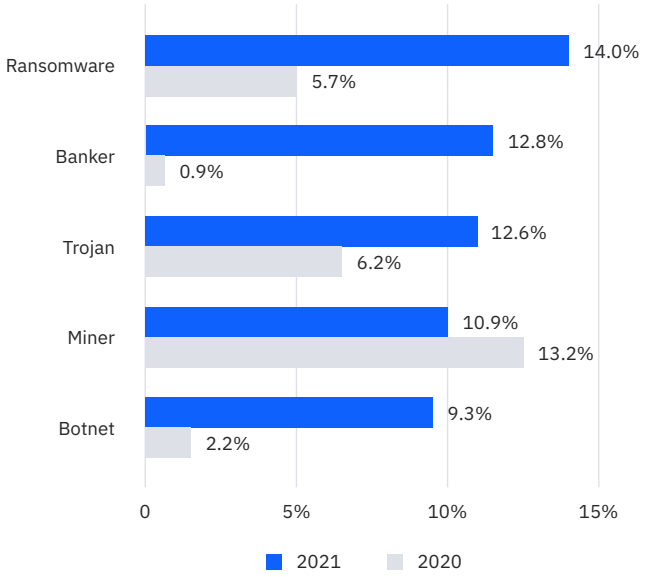
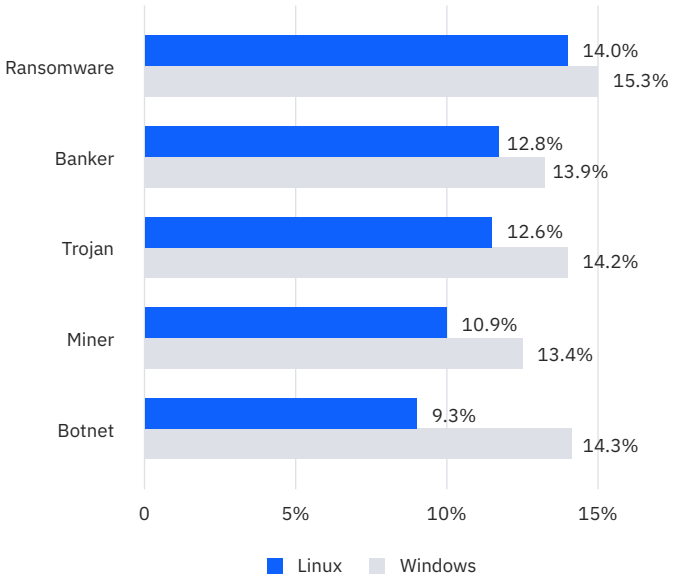


Figure 18

Malware with unique code, Linux vs. Windows, 2021

Comparison of new Linux malware vs. new Windows malware, 2021 (Source: Intezer)



Threat actors target cloud environments

IBM research into the cloud security threat landscape highlighted threat actors' continued efforts to shift targeting into cloud environments. Data gathered showed that threat actors used a variety of methods to gain initial access into organizations' cloud assets, with nearly a quarter of incidents stemming from threat actors pivoting into the cloud from on-premise networks. In addition, API misconfiguration issues were involved in nearly two-thirds of studied incidents. This targeting coincided with a robust underground marketplace for cloud-related credentials, with tens of thousands of accounts for sale online.

As organizations move into the cloud, threat actors are following right alongside. Maintaining properly hardened systems, enacting effective password policies, and ensuring policy compliance is critical to maintaining a robust cloud security posture.

Fileless malware in the cloud

Evasive, fileless malware lurking in memory can elude standard detection tools by exploiting legitimate scripting languages and sidestepping the use of signatures. X-Force research has found that, besides using scripts to launch fileless malware, threat actors are now using Ezuri, an opensource crypter and memory loader written in Golang, which makes it even easier to launch undetected malware.

X-Force research has also highlighted the development of a new malware suite dubbed VermillionStrike. VermillionStrike is based on the popular penetration testing tool CobaltStrike; however, unlike its counterpart, VermillionStrike is designed to run on Linux systems. This development highlights the continued migration to malware targeting Linux, and likely indicates ongoing operations outside of Windows environments will continue into the future.

Geographic trends

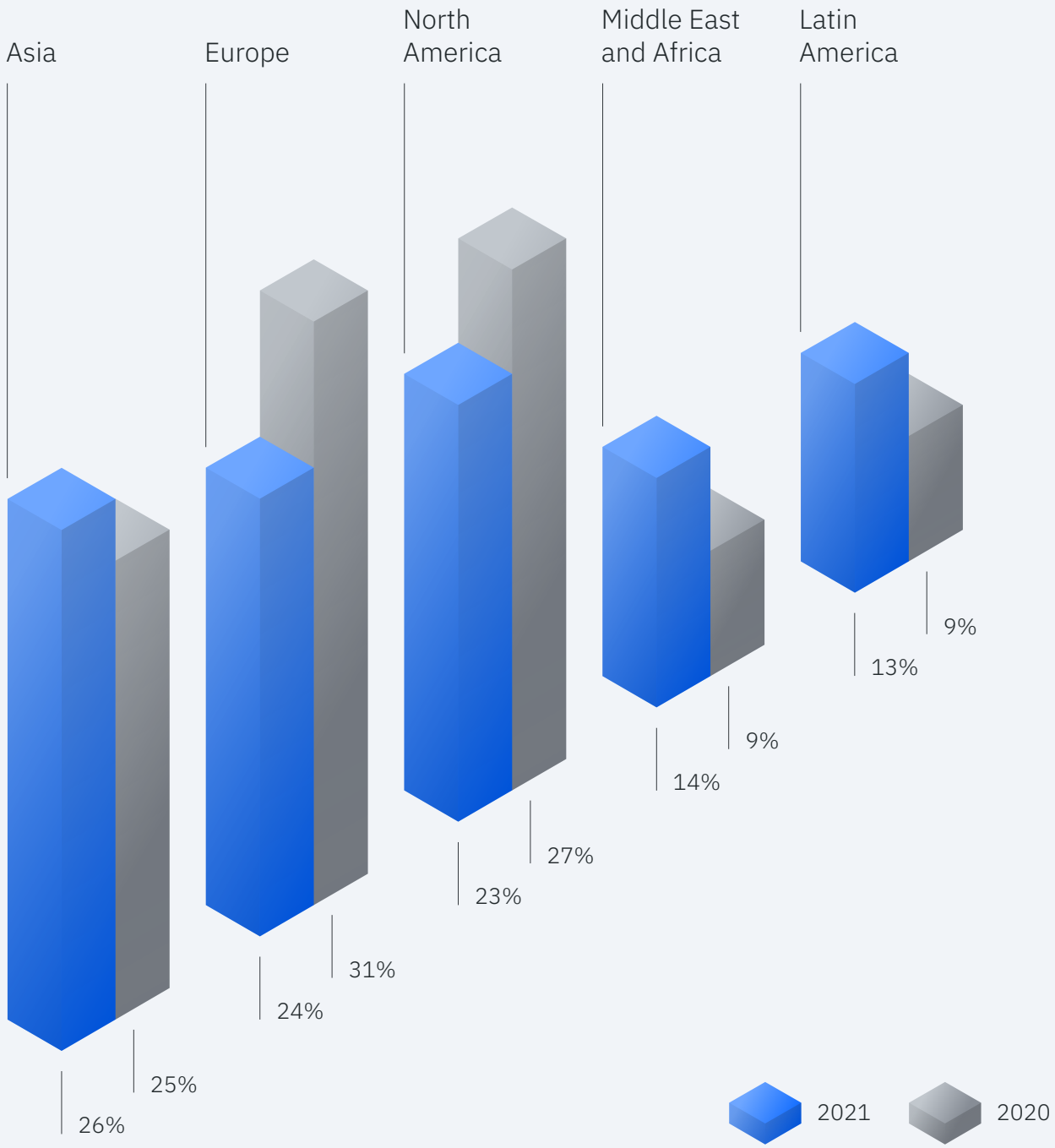
For the first time since this report began documenting geographic trends, Asia has moved into first place as the most-attacked region in 2021, receiving 26% of attacks X-Force observed last year. A flurry of attacks on Japan in particular—potentially related to the Summer Olympic Games held in Japan in 2021—appear to have contributed to this attack trend.

Europe and North America followed closely behind, garnering 24% and 23% of attacks respectively, and the Middle East and Africa and Latin America received 14% and 13% of attacks respectively.

Figure 19

Breakdown of attacks by geography, 2021 vs. 2020

Source: IBM Security X-Force



Asia

For the purposes of reporting, IBM considers Asia to include Australia, East and Southeast Asia, India, and the Pacific islands.

Server access attacks (20%) and ransomware (11%) were the top two attack types on Asian organizations in 2021, followed closely by data theft (10%). The high percentage of server access attacks in Asia suggests that Asian organizations are adept at identifying attacks quickly before they escalate into more concerning attack types. Remote access trojans and adware tied for fourth place, at 9% of attacks.

In Asia, REvil made up 33% of ransomware attacks X-Force observed, and Bitlocker, Nefilim, MedusaLocker and Ragnar Locker were significant players as well.

Vulnerability exploitation and phishing tied for the top infection vector at Asian organizations in 2021, both leading to 43% of attacks observed in the region. Brute force (7%) and use of stolen credentials (7%) were also occasionally employed to gain initial access to networks.

In Asia, finance and insurance organizations were attacked most frequently, making up 30% of the incidents X-Force remediated, followed closely by manufacturing (29%) and then more distantly by professional and business services (13%) and transportation (10%). Globally, finance and insurance was the top-attacked industry X-Force observed from 2015-2020, so Asia experienced a continuation of this worldwide trend X-Force has observed for years.

Japan, Australia and India were the most-attacked countries in Asia.

Top attacked industries

1.	Finance and insurance	30%
2.	Manufacturing	29%
3.	Professional and business services	13%

Europe

For the purposes of reporting, IBM considers European organizations to be located in Western Europe, Eastern Europe, and Turkey.

Europe emerged as the second-most attacked region in the world, receiving 24% of the attacks X-Force incident response team observed. Ransomware was the top attack type for Europe, making up 26% of all attacks in the region in 2021. Server access (12%) came in second place, followed by data theft (10%), misconfiguration (8%), malicious insiders (6%) and fraud (6%). Ransomware attackers are potentially drawn by the number of high-revenue-generating organizations in Europe that might be potential targets for ransomware. REvil attacks made up 38% of ransomware attacks on Europe in 2021 and Ryuk another 25%. DarkSide, LockBit 2.0, and Crystal ransomware groups were also observed. These ransomware groups tend to pursue "big game hunting," or targeting significant portions of enterprise networks belonging to large, wealthy corporations with the end goal of a big ransom payout.

Vulnerability exploitation was the top infection vector used against European organizations, accounting for 46% of all incidents X-Force remediated in Europe, and followed closely by phishing at 42%. Brute force was used in 12% of incidents.

Manufacturing was the top attacked industry in Europe in 2021, with 25% of attacks, followed by finance and insurance (18%) and then professional and business services (15%). Ransomware attackers' focus on manufacturing and professional services organizations was probably driving these trends.

The United Kingdom, Italy, and Germany were the most-attacked countries in Europe.

Top attacked industries

1.	Manufacturing	25%
2.	Finance and insurance	18%
3.	Professional and business services	15%

North America

For the purposes of reporting, IBM considers North America to include the United States and Canada.

North America emerged as the third-most attacked region in the world in 2021, receiving 23% of the attacks X-Force incident response team observed. Similar to Europe, ransomware led as the top attack type on North American organizations, making up 30% of all attacks in this region. It's possible that the increased law enforcement activity in 2021, including the takedown of botnets and ransomware groups, are beginning to impede the attack rate we traditionally observed in the region.

REvil attacks made up 43% of the ransomware attacks X-Force observed in North America, and X-Force also observed LockBit 2.0, Conti, CryptoLocker and Eking. After ransomware, BEC was the second-most common attack type in North America, making up 12% of attacks and suggesting that BEC attackers have renewed their assault on North American organizations, seeking to compromise organizations that do not have MFA deployed. Server access attacks (9%) came in third place for North American organizations.

Phishing appears to be the attack vector of choice for threat actors targeting North America, observed in 47% of the incidents X-Force remediated in this region in 2021. Vulnerability exploitation came in second at 29%, and removable media (12%), brute force (9%) and stolen credentials (9%) were also used. Threat actors may be focused on phishing as more North American organizations implement robust patch management programs in the face of several critical vulnerabilities released in 2020 and 2021.

Manufacturing was the top-attacked industry in North America, constituting 28% of all attacks X-Force remediated—an attack rate probably associated with the significant supply chain-related strain on manufacturing emerging from the pandemic. Professional and business services came in second place at 15%, followed by retail and wholesale at 11%. Manufacturing, professional services and wholesale are all attractive targets for ransomware actors possibly due to their low tolerance for downtime and sensitive client data on their networks that—if stolen and threatened to be leaked—can put intense pressure on a victim to pay a ransom.

Top attacked industries

1.	Manufacturing	28%
2.	Professional and business services	15%
3.	Retail and wholesale	11%

Middle East and Africa

For the purposes of reporting, IBM considers the Middle East and Africa to include the Levant, Arabian Peninsula, Egypt, Iran and Iraq, and the entire African continent.

Ransomware and server access attacks were the top incident types for the Middle East and Africa, tying for first place with 18% of attacks each. Misconfiguration was a close second at 14%, and credential harvesting and DDoS attacks were also fairly common in the region.

Vulnerability exploitation led to 50% of the incidents X-Force remediated in the Middle East and Africa where the initial infection vector was known. Use of stolen credentials and phishing were also frequently used to gain access to Middle East and Africa networks of interest, and password spraying and use of removable media were occasionally used to gain initial access as well.

Finance and insurance organizations made up the overwhelming majority of targets in the Middle East and Africa in 2021, accounting for 48% of all attacks, signaling a potential shift from nation-state sponsored energy-focused attacks in the region to cybercriminal attacks focused on financial organizations. Saudi Arabia's shift to diversify its economy away from crude revenues may also be impacting this trend. Healthcare organizations made up another 15% of attacks in the region, and energy organizations were associated with 10% of attacks in the region.

Saudi Arabia, the United Arab Emirates, and South Africa were the most-attacked countries in the Middle East and Africa region.

Top attacked industries

1.	Finance and insurance	48%
2.	Healthcare	15%
3.	Energy	10%

Latin America

For the purposes of reporting, IBM considers Latin America to include Mexico, Central America and South America.

The top attack type for Latin America in 2021 was ransomware, making up 29% of attacks, followed by BEC (21%) and credential harvesting (21%), tying for second place. REvil was the most common ransomware strain observed in Latin America, making up 50% of ransomware attacks X-Force remediated, with Ryuk and AtomSilo also being observed targeting organizations in the region. As discussed previously in this document, the rate of BEC attacks against Latin America is higher than for any other geography, and represents a sharp increase since 2019, suggesting that BEC attackers are focusing greater attention on Latin American targets.

Phishing was the most common infection vector threat actors used against Latin American targets, making up 47% of attacks X-Force remediated in this region. The high number of BEC attacks and ransomware attacks delivered via phishing is probably driving this trend. Stolen credentials led to 29% of attacks on Latin American organizations, and this high percentage compared to other regions suggests that more widespread use of MFA could help to drive down stolen credential and BEC incidents in this region. Vulnerability exploitation led to only 18% of incidents at Latin American organizations while removable media accounted for another 6%.

Manufacturing was the most-targeted industry in Latin America in 2021, but at 22% led by only a small margin. Retail and wholesale (20%), finance and insurance (15%), and perhaps most surprisingly, mining (11%) followed closely behind. Professional and business services and energy were also fairly heavily attacked in Latin America. Ransomware attackers and BEC attackers appear to be interested in targeting these industries, probably driving the attack rate for these industries in Latin America.

Brazil, Mexico and Peru were the most-attacked countries in Latin America.

Top attacked industries

1.	Manufacturing	22%
2.	Retail and wholesale	20%
3.	Finance and insurance	15%

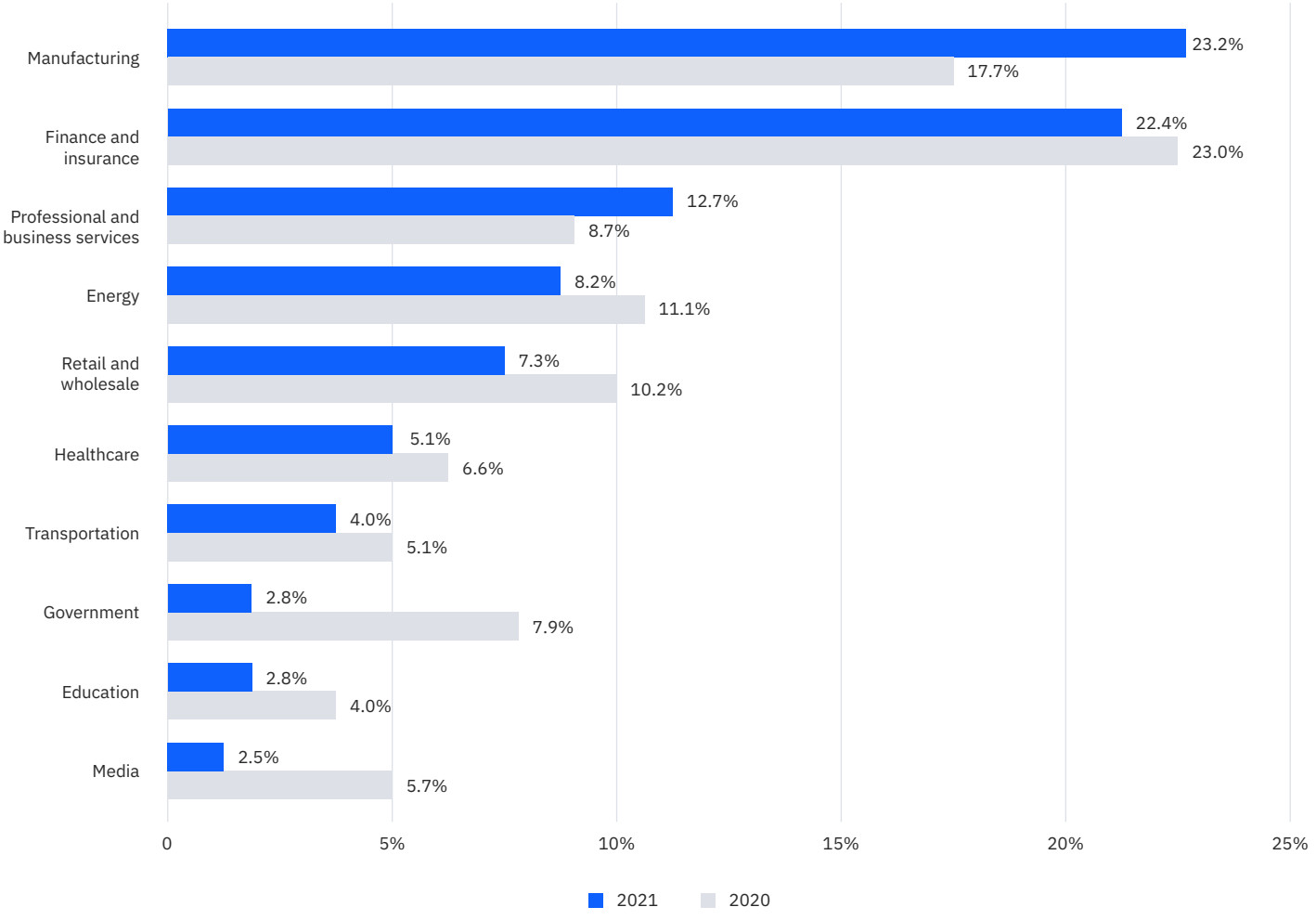
For the first time in over five years of this report, finance and insurance was not the top-attacked industry in 2021, as manufacturing overtook it by a slight margin. The onslaught of ransomware and BEC attacks targeting manufacturing organizations—compounding supply chain pressure created by the COVID-19 pandemic—possibly contributed to this shift.

In addition to finance and manufacturing, professional and business services was heavily targeted in 2021, particularly by ransomware actors. This year, we are combining professional and business services as well as retail and wholesale to provide a broader picture of the industry attack landscape. It is worth noting that wholesale was much more heavily attacked than retail last year, with wholesale largely driving the ranking for this industry group. We wanted to ensure the attack level against wholesale was captured in this year's rankings.

Figure 20

Breakdown of attacks on the top 10 industries, 2021 vs. 2020

(Source: IBM Security X-Force)



#1 | Manufacturing

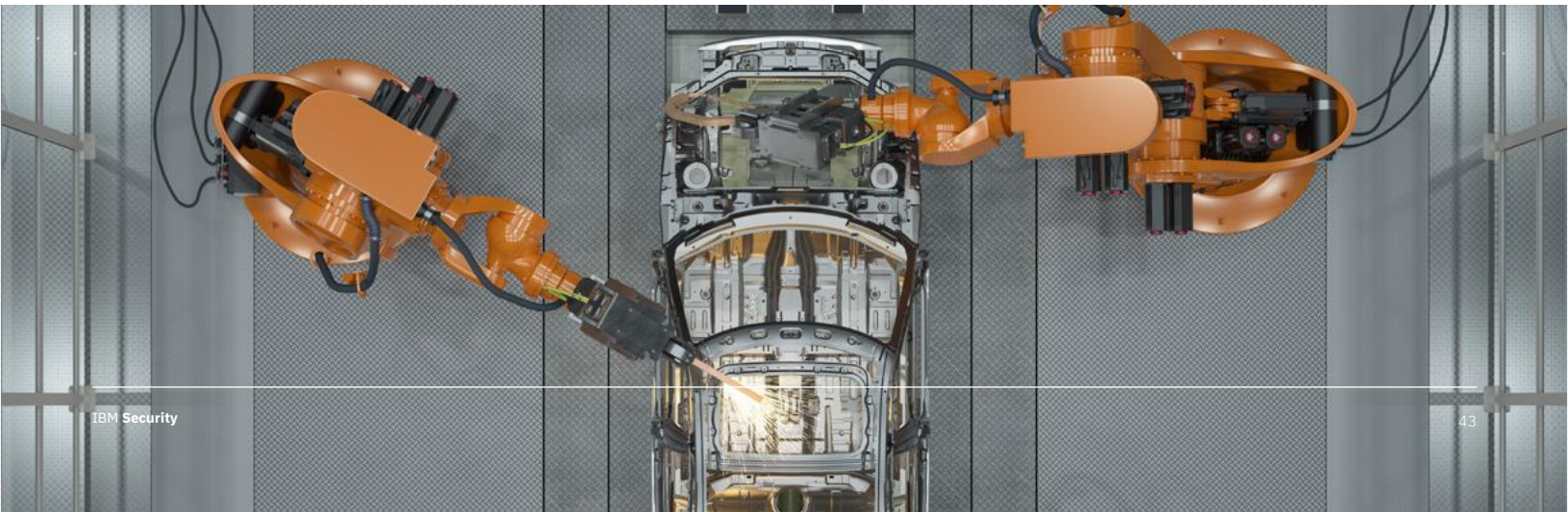
Taking first place in X-Force's ranking for the first time since 2016, manufacturing was the top attacked industry in 2021, targeted in 23.2% of the attacks X-Force remediated.

23.2%
of attacks

Ransomware was the top attack type, accounting for 23% of attacks on manufacturing organizations and underscoring the heavy focus ransomware actors placed on manufacturing. Server access attacks came in second place at 12%, representing probably some failed attacker operations. BEC and data theft tied for third place, at 10% each. BEC attackers are probably seeking to capitalize on the many supplier, sub-supplier, and wholesale shipping relationships manufacturing organizations develop, and attempt to redirect payments between partners to accounts under the BEC attackers' control. Data theft probably aims at stealing sensitive intellectual property or holding data for ransom.

Vulnerability exploitation was the top infection vector at manufacturing organizations in 2021, at 47%, followed closely by phishing at 40%. The volume of these attacks probably drove the overall initial infection vector trends X-Force observed in 2021. Removable media (7%), stolen credentials (3%) and brute force (3%) also accounted for a small percentage of attacks. Although vulnerability exploitation came out on top, manufacturing organizations will probably want to devote an equal amount of effort to combating phishing threats, in addition to vulnerability management.

Nearly one-third, or 32% of attacks on manufacturing organizations occurred in Asia in 2021, with North America (27%) and Europe (26%) seeing similar percentages of attacks. Latin America (13%) and the Middle East and Africa (5%) also saw attacks on manufacturing in their region.



#2 | Finance and insurance

Finance and insurance organizations were in the crosshairs of 22.4% of attacks X-Force remediated in 2021, placing it solidly in second place within X-Force's industry rankings. Of these attacks, 70% were on banks, 16% were on insurance organizations, and 14% were on other financial organizations.

22.4%

of attacks

The financial industry's drop from first place suggests that the high security standards in place at most financial organizations are yielding concrete results and that the financial services industry is doing security right. In addition, hybrid cloud environments are dominant at financial services organizations, allowing for better visibility into and management of sensitive data.

Server access attacks narrowly emerged as the top attack type on finance and insurance organizations in 2021, making up 14% of all attacks. This was followed closely by ransomware, misconfigurations, and fraud, which all tied for second place at 10%. RATs, adware and credential harvesting were also fairly common attack types against financial services.

Phishing was the most common infection vector for financial services, leading to 46% of attacks against this sector in 2021. Vulnerability exploitation came in second place, leading to 31% of attacks on this sector. Password spraying, brute force and VPN access were also observed infection vectors against finance and insurance firms.

Asia saw a high volume of attacks on finance and insurance organizations in 2021—34% of all attacks on this industry. Finance and insurance attacks in the Middle East and Africa were also disproportionately large, at 29%, while Europe (19%), North America (9%), and Latin America (9%) saw moderately small shares of the attacks on finance and insurance in 2021.

#3 | Professional and business services

12.7%

of attacks

Professional services include information technology providers, law firms, architects, accountants, and specialist consultants. Business services include firms such as office administration, human resources, security services, travel arrangements, and landscaping. Together they form a larger services industry we are including for the 2022 X-Force Threat Intelligence Index.

Professional and businesses services firms were third-most attacked in our 2022 ranking, accounting for 12.7% of all attacks we observed. Of these, 24% were business services firms, 76% were professional services firms, and 29% were specifically information technology-focused professional services providers.

Ransomware was the top attack type against professional and business services firms in 2021, making up 32% of all attacks X-Force observed on these industries. Server access attacks were the second-most common attack type (19%), and an increase in server access attacks in Q4 2021 coinciding with a decrease in ransomware attacks in Q4 suggests that professional services firms did a better job at identifying and stopping ransomware attackers before they met their objectives. Malicious insiders came in third place at 13% of all attacks on the professional and business services industries.

Vulnerability exploitation accounted for 50% of incidents X-Force remediated at professional and business services firms in 2021, with phishing making up another 20%. Use of stolen credentials accounted for another 20% of the incidents we remediated in this sector. Multiple vulnerability exploitation incidents involved threat actors taking advantage of the Microsoft Exchange vulnerabilities revealed early in 2021.

#4 | Energy

Energy organizations were fourth-most attacked in this year's rankings, experiencing 8.2% of attacks observed and dropping from third place the year prior. It is possible that following the blowback from the DarkSide ransomware attack on Colonial Pipeline in May 2021, threat actors—and specifically ransomware actors—shifted their focus away from energy organizations for fear of retaliation. In 2021, X-Force observed fewer incidents against energy organizations in all of June, July and August than in May, when Colonial Pipeline occurred. Attacks appeared to pick back up again in September, however.

8.2%

of attacks

Ransomware (25%) was the most common attack type against energy organizations in 2021, followed by RATs, DDoS and BEC, all of which tied for second place (17%). Botnets, spam and data theft also played a role against energy firms in 2021.

Phishing was the most common infection vector threat actors used to gain access to energy organizations' networks, making up around 60% of attacks, while vulnerability exploitation made up the other 40% of incidents.

North America saw more attacks on energy organizations than any other region, claiming 31% of all energy attacks X-Force observed last year, with Europe coming in at 28%, Latin America and the Middle East and Africa tying for second at 17% and Asia last with 7% of attacks on energy.

#5 | Retail and wholesale

Retail establishments focus on the sale of finished goods directly to consumers while wholesale organizations focus on distributing and transporting goods directly from manufacturers, usually to a third party or directly to consumers. These industries were the fifth-most targeted in X-Force's 2022 ranking, accounting for 7.3% of all attacks in 2021. Of these, 35% were on retail and 65% were on wholesale, underscoring the strong emphasis threat actors placed on wholesale organizations last year, possibly due to the critical role they play in supply chains and movement of goods from manufacturers to end users.

7.3%

of attacks

BEC, server access, data theft, and credential harvesting were the top attack types on retail and wholesale last year. Ransomware and banking trojans also accounted for a high percentage of attacks, followed by RATs, misconfiguration, and fraud.

Phishing was the top infection vector for retail and wholesale in 2021, accounting for 38% of the attacks X-Force remediated in this industry where the initial infection vector was known. Stolen credentials came in second at 31%, and vulnerability exploitation made up another 23% of attacks on these industries. Brute force (8%) also played a role in some attacks.

North America and Latin America tied for the highest number of incidents in the retail and wholesale industries in 2021, both claiming 35% each, and Europe was close behind at 31%.

#6 | Healthcare

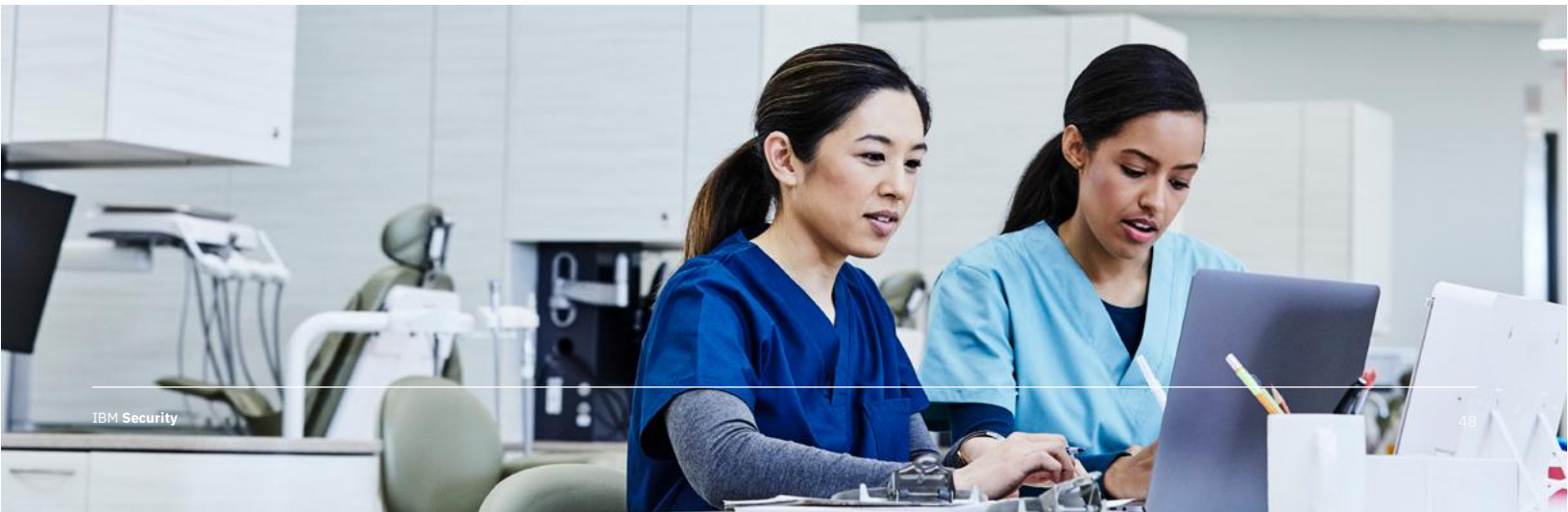
Healthcare emerged as sixth-most attacked in this year's rankings, receiving 5.1% of all attacks X-Force observed in 2021 and up from seventh place the year prior. Of attacks on healthcare where the attack type is known, 38% were ransomware—a higher percentage than most other industries. AtomSilo, AvosLocker and REvil ransomware actors all targeted healthcare organizations this year. In addition to ransomware, BEC attacks (25%) hit the healthcare industry fairly hard this year, and server access, credential harvesting and misconfigurations also had an effect.

5.1%

of attacks

Vulnerability exploitation was the top infection vector at healthcare organizations in 2021, leading to 57% of the incidents X-Force remediated, followed by phishing at 29% and use of stolen credentials at 14%.

Healthcare organizations in the Middle East and Africa emerged as the most attacked in 2021, accounting for a massive 39% of attacks on healthcare, followed closely by North America at 33%. Asia and Latin America tied at 11% with Europe taking only 6% of healthcare attacks.



#7 | Transportation

The transportation industry received 4.0% of attacks, bringing it to the seventh ranking, up from ninth place in 2020. As international borders and transportation networks reopened in 2021, renewed activity in this industry is probably attracting renewed attacker interest.

4.0%

of attacks

Malicious insiders emerged as the top attack type against transportation organizations in 2021, making up 29% of attacks on this industry. Ransomware, RATs, data theft, credential harvesting and server access attacks all played a role against transportation in 2021 as well.

Half of all incidents X-Force remediated at transportation organizations in 2021 were initially caused by a phishing email, followed by use of stolen credentials at 33% and vulnerability exploitation at 17%.

Asia by far saw the bulk of attacks within the transportation industry, accounting for 64% of X-Force incidents in this sector in 2021, followed by Europe (21%), the Middle East and Africa (7%), and North America (7%).

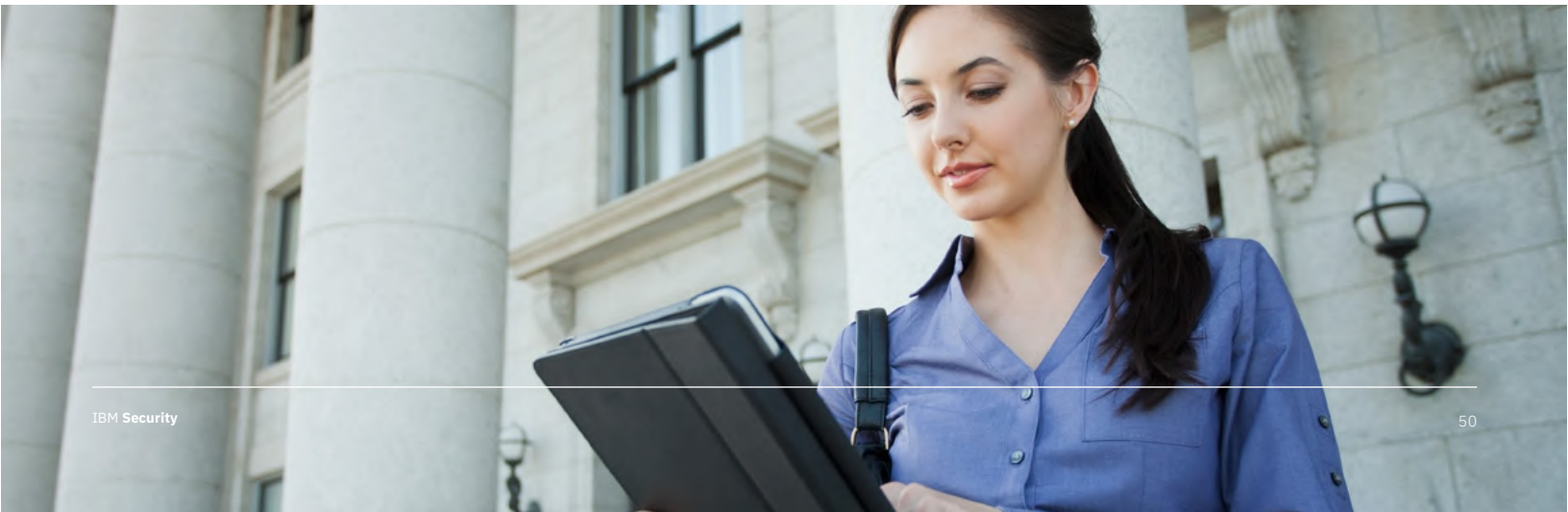
#8 | Government

The government sector along with education tied for eighth most targeted in 2021, experiencing 2.8% of attacks. Server access attacks were the most common attack type against the public sector last year, suggesting that X-Force's government clients in 2021 were particularly adept at identifying and eradicating threat actors from their network before the actors moved beyond server access. Data theft and fraud rounded out the top three attack types for government in 2021. Vulnerability exploitation was the most common infection vector used against government targets, followed by phishing.

Government targeting was spread geographically, with half of all attacks in Asia followed closely by North America at 30%. The Middle East and Africa (10%) and Europe (10%) saw some targeting against government organizations as well.

2.8%

of attacks



#9 | Education

Education organizations received 2.8% of attacks in 2021 based on X-Force's research, thus tying for eighth place with the government sector. Adware was the most common attack type observed against Education organizations in 2021, making up 33% of attacks, followed closely by ransomware at 22%. BEC, RATs, server access attacks and fraud were also commonly seen at education organizations last year.

Phishing was the top infection vector threat actors used against education, followed by brute force attacks. Asia was the most-attacked region in terms of incidents against education organizations in 2021, followed by North America.

2.8%

of attacks

#10 | Media

Media, which includes telecommunications, news outlets, publishers, and movie production, accounted for 2.5% of attacks in 2021, rounding out the top 10 most attacked industries. Ransomware was the top attack type observed against media outlets, making up 33% of all attacks X-Force observed in this sector, followed by server access, RAT, cryptomining, and malicious insider incidents. Brute force and stolen credentials are the primary methods X-Force observed attackers using to breach media organizations, suggesting that robust implementation of MFA might insulate this sector from several attack types. Europe and Latin America saw the largest share of attacks within the media industry, but attacks on media also occurred in the Middle East and Africa, North America, and Asia.

2.5%

of attacks

Risk mitigation recommendations

The threats we have presented in this report have the potential to cause concern, as the report underscores the grave and increasing threat from ransomware, renewed threats from BEC and phishing, and highlights several zero-day exploits threat actors have exploited over the past year. However, our intention is for this information to empower organizations as they better understand the current threat landscape, and help build confidence in the actions they need to take to combat these threats.

Some security principles X-Force has found helpful in combating today's cyber threats include a zero trust approach, automation of incident response, and extended detection and response capabilities.

Zero trust assists in decreasing risk of top attacks

Zero trust is a paradigm shift, a new way of approaching security problems, that assumes a breach has already happened and aims to increase the difficulty for an attacker to move throughout a network. At its core is understanding where critical data resides and who has access to this data, and creating robust verification measures throughout a network to ensure only the right individuals are accessing that data in the right way.

Research by X-Force threat researchers confirms that principles related to a zero trust approach—to include implementation of MFA and the principle of least privilege—have the potential to decrease organizations' susceptibility to the top attack types identified in this report, particularly ransomware and BEC.

Applying the principle of least privilege to domain controllers and domain administrator accounts in particular can increase barriers for ransomware actors, as many of these actors seek to deploy ransomware to a network from a compromised domain controller. In addition, implementing MFA increases the difficulty for cybercriminals seeking to take over email accounts by requiring that they provide further authentication beyond stolen credentials.

Learn more about how to build a zero trust approach →

Security automation enhances incident response

The X-Force incident response team addresses hundreds of incidents every year, in a variety of geographies, assisting in-house incident response analysts and addressing a range of attack types. Speed is of the essence, whether that means identifying and eradicating threat actors before they can deploy ransomware on a network, or quickly and efficiently resolving issues to create bandwidth for the next incident. In this fast-paced environment, security automation is key—outsourcing to machines tasks that might take a human analyst or team hours, and identifying mechanisms for improving workflows.

In mid-2021, IBM donated a threat hunting automation tool to the Open Cybersecurity Alliance, aimed at assisting security operations center (SOC) analysts to quickly conduct forensic investigations and address cyber incidents. In addition, the X-Force IR team uses IBM Security QRadar SOAR to enhance its incident response capabilities.

Learn more about IBM's incident response services →

Extended detection and response provides a significant advantage over attackers

Detection and response technologies—particularly when several different solutions are combined into an extended detection and response (XDR) solution—provide organizations with a significant advantage in identifying and eradicating attackers from a network before they are able to reach the final stage of their attack, such as ransomware deployment or data theft.

In multiple instances, when the X-Force IR team has deployed an endpoint detection and response (EDR) or XDR solution on a client's network, IR has immediately gained additional insight that has assisted in identifying attacker activities and quickly addressed them. XDR technologies are probably helping to drive the increase in server access and other attack types X-Force observes that indicate an attacker was identified and stopped before the operation could achieve its intended conclusion.

Learn more about IBM Security QRadar XDR →

Recommendations

The following recommendations include specific actions organizations can take to better secure their networks against the threats presented in this report.

Develop a response plan for ransomware. Every industry and every geography is at risk of a ransomware attack, and how your team responds in the critical moment can make all the difference in the amount of time and money lost in a response.

- Include in your response plan immediate containment actions, what stakeholders and law enforcement officials should be informed, how your organization will safely store and restore from backups, and an alternate location from where critical business functions can be run during remediation.
- Include in your plan a scenario of data theft and leak as part of the ransomware attack—this is a very common tactic used today, seen in a very high percentage of ransomware attacks X-Force remediates.
- Use ransomware drills to also think through whether your organization would pay a ransom and what factors would alter your calculus for that decision.
- Ensure your ransomware response plan includes a specific contingency for a cloud-related incident, as it may require additional tools and skills.
- Avoid data corruption due to malware or ransomware attacks with flash storage solutions that help prevent data loss, promote operational continuity, and lower infrastructure costs.
- X-Force's Definitive Guide to Ransomware gives additional detailed advice on how to respond to a ransomware attack. X-Force's incident response team can also conduct a ransomware readiness assessment for your organization to help build and test a ransomware incident response plan. The X-Force Command Center similarly prepares organizations for a ransomware attack, taking into account both the business and technical response required.

Implement multifactor authentication on every remote access point into a network. X-Force has observed more organizations implementing MFA more successfully than ever before. This is literally altering the threat landscape, forcing threat actors to find new ways of compromising networks rather than leveraging stolen credentials, and decreasing the effectiveness of email takeover campaigns.

- MFA can decrease the risk of several different attack types, including ransomware, data theft, BEC, and server access.
- In addition, identity and access management technologies are making MFA implementation easier every year—both for implementation teams and for end-users.

Adopt a layered approach to combat phishing. Unfortunately, there is no one tool or solution that will prevent all phishing attacks today, and threat actors continue to refine social engineering and anti-malware detection techniques to circumvent established controls. Thus, we recommend implementing several layers of solutions that have a higher chance of catching phishing emails.

— First, effective user awareness and education is key and should include real-world examples.

— Second, employ an email software security solution to put a machine to the task of identifying and filtering out malicious messages.

— Third, implement several defenses that can help to catch malware or lateral movement quickly should a phishing email slip through, including behavioral-based anti-malware detection, endpoint detection and response (EDR), intrusion detection and prevention solutions (IDPS), and a security information and event management (SIEM) system.

Refine and mature your vulnerability management system. Vulnerability management is an art—from identifying which vulnerabilities are most applicable to your organization's network architecture, to identifying how to deploy them without breaking anything in the process.

— Having a team dedicated to vulnerability management and making sure this team is well-resourced and supported can make all the difference in ensuring your network is protected from potential vulnerability exploitation.

— We recommend prioritizing any of the vulnerabilities mentioned in this assessment that are applicable to your organization.

— IBM's X-Force Exchange also includes a repository of vulnerabilities and associated criticality levels to assist you in identifying vulnerabilities of most concern, and X-Force Red can provide specialized vulnerability scanning and management services.

About IBM Security X-Force

IBM Security X-Force is a threat-centric team of hackers, responders, researchers and analysts. Our portfolio includes offensive and defensive products and services, fueled by a 360-degree view of threats. With X-Force as your security partner, you can affirm with confidence that the likelihood and impact of a data breach are minimal.

IBM Security X-Force Threat Intelligence combines IBM security operations telemetry, research, incident response investigations, commercial data, and open sources to aid clients in understanding emerging threats and quickly making informed security decisions.

Additionally, the X-Force Incident Response team provides detection, response, remediation, and preparedness services to help you minimize the impact of a data breach.

X-Force combined with the IBM Security Command Center experiences trains your team—from analysts to the C-suite—to be ready for the realities of today's threats. X-Force Red, IBM Security's team of hackers, provides offensive security services, including penetration testing, vulnerability management and adversary simulation.

Throughout the year, IBM X-Force researchers also provide ongoing research and analysis in the form of blogs, white papers, webinars and podcasts, highlighting our insight into advanced threat actors, new malware, and new attack methods. In addition, we provide a large body of current, cutting-edge analysis to subscription clients through our X-Force Threat Intelligence solutions.

Schedule a consultation with one of our X-Force experts

About IBM Security

IBM Security works with you to help protect your business with an advanced and integrated portfolio of enterprise security products and services, infused with AI and a modern approach to your security strategy using zero trust principles—helping you thrive in the face of uncertainty. By aligning your security strategy to your business; integrating solutions designed to protect your digital users, assets, and data; and deploying technology to manage your defenses against growing threats, we help you to manage and govern risk that supports today's hybrid cloud environments.

Our new modern, open approach, the IBM Cloud Pak for Security platform, is built on RedHat Open Shift and supports today's hybrid multicloud environments with an extensive partner ecosystem. Cloud Pak for Security is an enterprise-ready containerized software solution that enables you to manage the security of your data and applications—by quickly integrating your existing security tools to generate deeper insights into threats across hybrid cloud environments—leaving your data where it is, allowing easy orchestration and automation of your security response.

For more information, please check out www.ibm.com/security or visit the IBM Security Intelligence blog.

Contributors

Camille Singleton
Charles DeBeck
Joshua Chung
Dave McMillen
Scott Craig
Scott Moore
Charlotte Hammond
John Dwyer
Melissa Frydrych
Ole Villadsen
Richard Emerson
Guy-Vincent Jourdan
Vio Onut
Stephanie Carruthers
Adam Laurie
Michelle Alvarez
Salina Wuttke
Georgia Prassinos
John Zorabedian
Mitch Mayne
Limor Kessem
Ian Gallagher
Ari Eitan

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2022